

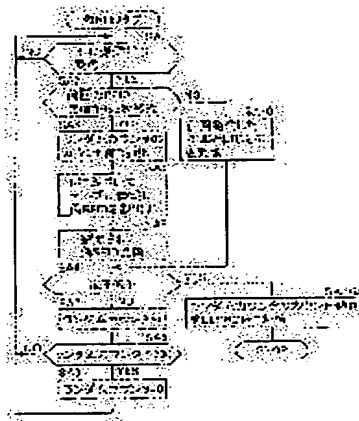
(43) Date of publication of application : 08.07.2004

G06K 19/073
G06F 12/14
G06F 17/60
G06K 17/00
G06K 19/07
H04L 9/32

(72)Inventor : TSUKAMOTO YUTAKA

PROBLEM TO BE SOLVED: To prevent an invasion of privacy based on a specific identifier read in.

SOLUTION: An individual user is provided with a false identifier (RFID) transmitter for transmitting a disturbing false RFID to an invader. On the reception of a command to transmit an RFID from a tag reader (SA1), a variable false RFID different from the one in the preceding transmission is transmitted (SA3 to SA5), so that the same person transmits a different RFID every time. False RFID transmitters are grouped into a plurality of types, and false RFID transmitters of the same group transmit the same common false RFID with high probability although transmitting individual variable false RFIDs respectively. Individual users are provided with a group of false RFID transmitters assigned to their area, so that different persons transmit the same RFID in some cases.



[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-192645

(P2004-192645A)

(43) 公開日 平成16年7月8日 (2004.7.8)

(51) Int. Cl. ⁷

F I

テーマコード (参考)

G06K 19/073

G06K 19/00

P

5B017

G06F 12/14

G06F 12/14

320A

5B035

G06F 17/60

G06F 17/60

118

5B058

G06K 17/00

G06K 17/00

E

5J104

G06K 19/07

G06K 17/00

L

審査請求 未請求 請求項の数 33 O L 公開請求 (全 103 頁) 最終頁に続く

(21) 出願番号

特願2003-408568 (P2003-408568)

(22) 出願日

平成15年12月8日 (2003.12.8)

(71) 出願人 502178126

石井 美恵子

岡山県倉敷市羽島221番地の4

(74) 代理人 100104433

弁理士 宮園 博一

(72) 発明者 塚本 豊

京都府京都市下京区松原通東洞院東入本燈

電町11番地 デリート烏丸東50

4号室

Fターム(参考) 5B017 AA07 BA07

5B035 BB09 BC00 CA23

5B058 CA15 KA02 YA20

5J104 NA36 NA38

(54) 【発明の名称】 プライバシー保護方法、プライバシー保護用識別子発信装置、プライバシー保護システムおよびプログラム

(57) 【要約】

【課題】

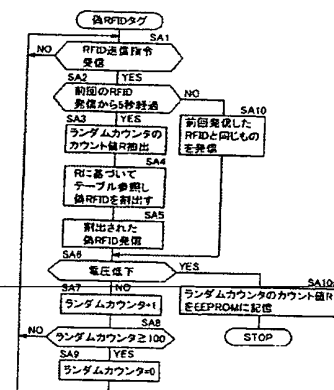
読取られた固有の識別子に基づいて行われるプライバシーの侵害を防止する。

【解決手段】

侵害者に対し攪乱用の偽識別子 (RFID) を発信する偽RFID発信装置を個人ユーザに提供し、タグリーダからのRFIDの送信指令を受信した場合に (SA1)、前回発信したものと異なる可変型の偽RFIDを発信し (SA3~SA5)、同一人物でありながらも毎回異なったRFIDを発信する。各偽RFID発信装置は複数種類にグループ化されており、同一グループに属する偽RFID発信装置同士はそれぞれ独自の可変型の偽RFIDを発信しながらも互いに一致する共通の偽RFIDを発信する確率を高めている。グループ毎に地域を指定して各偽RFID発信装置を個人ユーザに提供することにより、異なった人物でありながらも同一のRFIDが発信される場合出現させる。

【選択図】

図11



【特許請求の範囲】

【請求項 1】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、

前記個人ユーザに所持されるプライバシー保護用識別子発信装置により、偽識別子を生成する偽識別子生成ステップと、

識別子の送信要求があった場合に、前記偽識別子生成ステップにより生成された前記偽識別子を前記プライバシー保護用識別子発信装置から発信する発信ステップと、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取りステップとを含み、

前記偽識別子生成ステップは、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成ステップを含むことを特徴とする、プライバシー保護方法。

【請求項 2】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置を複数の個人ユーザに提供する提供ステップを含み

20

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段と、

識別子の送信要求があった場合に、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成して発信する前記プライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持する前記プライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能であり、

30

前記複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に前記共通の偽識別子が異なる複数のグループに分類され、

前記提供ステップは、前記それぞれのグループ毎に地域を指定して該グループに属する前記プライバシー保護用識別子発信装置を個人ユーザに提供することを特徴とする、プライバシー保護方法。

【請求項 3】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置を複数の個人ユーザに提供する提供ステップを含み

40

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段と、

識別子の送信要求があった場合に、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生

50

成可能であり、

前記提供ステップにより或る個人ユーザに提供されたプライバシー保護用識別子発信装置から、予め定められた所定個数の偽識別子を1度に発信し、

前記提供ステップにより前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から、前記所定個数よりも多い複数の偽識別子を1度に発信し、該複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成することを特徴とする、プライバシー保護方法。

【請求項4】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段と、

識別子の送信要求があった場合に、前記可変型偽識別子生成手段により生成された偽識別子を送信する発信手段とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【請求項5】

前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で前記偽識別子を生成することを特徴とする、請求項4に記載のプライバシー保護用識別子発信装置。

【請求項6】

前記発信手段は、前回の偽識別子の発信から所定時間内に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を送信することを特徴とする、請求項4または請求項5に記載のプライバシー保護用識別子発信装置。

【請求項7】

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能であることを特徴とする、請求項4～請求項6のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項8】

他のプライバシー保護用識別子発信装置と交信する交信手段をさらに含み、

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段を含み、

前記交信手段は、前記他のプライバシー保護用識別子発信装置と交信して、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信するとともに当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成することを特徴とする、請求項7に記載のプライバシー保護用識別子発信装置。

【請求項9】

前記交信手段は、互いの識別子を交換するときの交信可能通信限界距離が20メートル以内に定められており、該交信可能通信限界距離圏内に進入した他のプライバシー保護用識別子発信装置と交信して互いの識別子を交換することを特徴とする、請求項8に記載のプライバシー保護用固有識別子発信装置。

【請求項10】

前記交信手段は、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度前記識別子の交換を行なうことを禁止する禁止手段を有することを特徴とする、請求項8または請求項9に記載のプライバシー保護用識別子発信装置。

【請求項11】

前記交信手段は、電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成することを特徴とする、請求項 8 ～ 請求項 10 のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項 12】

前記交信手段は、電子メール機能を有しており、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読出すことにより前記共通の偽識別子として生成することを特徴とする、請求項 8 ～ 請求項 11 のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項 13】

前記発信手段は、他のプライバシー保護用識別子発信装置から 1 度に発信される所定個数の偽識別子よりも多い複数の偽識別子を 1 度に発信可能であり、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成することを特徴とする、請求項 4 ～ 請求項 12 のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項 14】

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段とを、さらに含むことを特徴とする、請求項 4 ～ 請求項 13 のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項 15】

前記識別子ガード手段は、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にすることを特徴とする、請求項 14 に記載のプライバシー保護用識別子発信装置。

【請求項 16】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

個人ユーザのプライバシーを保護するために匿名を名乗り匿名ユーザとして行動するために作成された匿名と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なう登録処理ステップと、

前記匿名ユーザ用の電子証明書を発行する電子証明書発行ステップと、

前記匿名ユーザの住所を、該匿名に対応する個人ユーザとは異なった住所に設定するための住所設定ステップと、

所定の業者にユーザ登録するとき前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録ステップと、

識別子の送信要求があった場合に、前記個人ユーザに所持されるプライバシー保護用識別子発信装置から偽識別子を発信する発信ステップと、

前記ユーザ登録ステップにより前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段とを含み、

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする、プライバシー保護方法。

【請求項 17】

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合でないときであっても、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする、請求項 16 に記載のプライバシー保護方法。

【請求項 18】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

個人ユーザのプライバシーを保護するために匿名を名乗り匿名ユーザとして行動するために作成された匿名と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なう登録処理手段と、

所定の業者にユーザ登録するとき前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録手段と、

識別子の送信要求があった場合に、前記個人ユーザに所持されるプライバシー保護用識別子発信装置から偽識別子を発信する発信手段と、

前記ユーザ登録手段により前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段とを含み、

前記発信手段は、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする、プライバシー保護システム。

【請求項 19】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって、

所定の業者に対し個人ユーザが匿名を名乗り匿名ユーザとして行動する場合に前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段と

識別子の送信要求があった場合に偽識別子を発信する手段であって、前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する発信手段とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【請求項 20】

前記発信手段は、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする、請求項 19 に記載のプライバシー保護用識別子発信装置。

【請求項 21】

前記所定の業者は、商品を販売する販売店であり、

前記匿名用偽識別子記憶手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録した当該販売店に対応する匿名用偽識別子を記憶しており、

前記発信手段は、前記販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする、請求項 19 または請求項 20 に記載のプライバシー保護用識別子発信装置。

【請求項 22】

前記匿名用偽識別子記憶手段は、複数の前記業者に対応してそれぞれ異なった匿名用偽

識別子を記憶しており、

前記発信手段は、前記複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から選択して発信することを特徴とする、請求項 19～請求項 21 のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項 23】

固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプログラムであって、

プライバシー保護用識別子発信装置に設けられているコンピュータに、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段と、

識別子の送信要求があった場合に、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段と、

して機能させるための、プログラム。

【請求項 24】

前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で前記偽識別子を生成させることを特徴とする、請求項 23 に記載のプログラム。

【請求項 25】

前記発信手段は、前回の偽識別子の発信から所定時間内に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信させることを特徴とする、請求項 23 または請求項 24 に記載のプログラム。

【請求項 26】

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能にすることを特徴とする、請求項 23～請求項 25 のいずれかに記載のプログラム。

【請求項 27】

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段を含み、

前記他のプライバシー保護用識別子発信装置と交信して、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信させるとともに当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成させることを特徴とする、請求項 26 に記載のプログラム。

【請求項 28】

既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度前記識別子の交換を行なうことを禁止する禁止手段として機能させることを特徴とする、請求項 26 または請求項 27 に記載のプログラム。

【請求項 29】

電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成させることを特徴とする、請求項 26～請求項 28 のいずれかに記載のプログラム。

【請求項 30】

電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読み出すことにより前記共通の偽識別子として生成させることを特徴とする、請求項26～請求項29のいずれかに記載のプライバシー保護用識別子発信装置。

【請求項31】

前記発信手段は、他のプライバシー保護用識別子発信装置から1度に発信される所定個数の偽識別子よりも多い複数の偽識別子を1度に発信させることが可能であり、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成させることを特徴とする、請求項23～請求項30のいずれかに記載のプログラム。

【請求項32】

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段と、

して機能させるプログラムをさらに含むことを特徴とする、請求項23～請求項31のいずれかに記載のプログラム。

【請求項33】

前記識別子ガード手段は、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にさせることを特徴とする、請求項32に記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、たとえばICタグ(RFIDタグ)等から発信されたRFID(Radio Frequency Identification)等の固有の識別子が読取られて該固有の識別子に基づくプライバシーの侵害を防止するための、プライバシー保護方法、プライバシー保護用識別子発信装置、プライバシー保護システムおよびプログラムに関する。

【背景技術】

【0002】

メーカーで製造された商品が卸売業者等の中間流通業者に出荷された後小売店に入荷されるその商品の流通段階で当該商品を管理するために、その商品にRFIDタグを付するという提案がなされている(たとえば、特許文献1)。

【0003】

この背景技術では、メーカーからの出荷時、中間流通業者への入荷時、小売店での入荷時、消費者の購入時等の流通段階における要所要所において、商品に付されているRFIDタグに記憶されているRFIDをタグリーダが読取り、当該RFIDが正規に登録されている適性なものであるか否かをチェックし、商品が正しく流通しているか否かを監視する。

【0004】

また、例えば、デパート等の小売店で購入したRFIDタグ付きの商品を購入者が袋に詰め、その袋を持って小売店の通過ゲートを通る際に、その通過ゲートに設けられているタグリーダと購入商品に付されているRFIDタグとが交信し、RFIDタグから送信されてきたRFIDに基づいて各商品の価格を自動的に割出してその合計を算出し、購入者が所持している決済機能付の携帯電話やICカード等と交信して自動決済を行なう方法が提案されている(たとえば、特許文献2参照)。

【特許文献1】特開2000-169229

【特許文献2】特開2000-196555

【発明の開示】

【発明が解決しようとする課題】

【0005】

このように、種々の商品に付されたRFIDタグは、タグリーダからのRFID送信要求に応じて記憶しているRFIDを自動的に発信するために、商品が例えば眼鏡や指輪やイヤリングや腕時計等のように、常時身に付けて携帯される物の場合には、当該商品が個人ユーザに購入された後においても、タグリーダからのRFID送信要求に応じて当該個人ユーザが身に付けている商品のRFIDタグからRFIDが発信されることとなる。その結果、当該個人ユーザのプライバシーが侵害される虞が生ずる。

【0006】

たとえば、前述の自動決済を行うの際に、タグリーダからのRFID送信要求に応じて、購入者が身に付けている購入済み商品に付されているRFIDタグからもRFIDが発信されることとなる。

【0007】

その結果、たとえば或る個人ユーザアリスが、Aデパートの婦人服売り場のマタニティコーナーで岩田帯（腹帯）を購入してその商品に付されているRFIDタグをタグリーダに読み取らせて自動決済を行なった後、食器売り場で夫婦茶碗を購入してその商品に付されているRFIDタグをタグリーダに読取らせて自動決済を行なった場合には、その個人ユーザが常時携帯している購入済み商品に付されているRFIDタグも同時に読み取られることとなる。そのRFIDタグのRFIDが例えば、123456であった場合には、123456のRFIDを発信するRFIDタグの商品を常時携帯している同一人物が岩田帯（腹帯）を購入するとともに夫婦茶碗も購入したことがわかってしまい、その個人ユーザは、おそらく、結婚前に妊娠していることが推測できてしまう。

【0008】

しかも、RFIDタグのRFIDを利用した自動決済の際に、そのAデパートのポイントカードによるポイント加算処理も合わせて行なった場合には、そのポイントカードの新規発行時にユーザ登録している個人名（アリス）や住所等の個人情報がつきとめられ、前述したRFID123456を発するRFIDタグを常時携帯している人物はアリスであることが見破られてしまう。

【0009】

そこで、商品購入時にその商品に付されているRFIDタグのRFID発信機能を停止状態に切換えるようにし、購入済商品を消費者が身につけたとしても、その商品からRFIDが発信されることがないように構成することが考えられる。

【0010】

しかし、このように構成した場合には、購入済商品に付されたRFIDタグから発せられるRFIDを利用して種々のサービスを楽しむことができないという不都合が生ずる。購入済み商品のRFIDタグのRFIDを利用したサービスとしては、例えば、商品のRFIDタグから発せられるRFID毎に分類して当該商品の詳細な情報を登録しているサーバに消費者がRFIDのコードを送信してアクセスし、当該RFIDに対応する商品情報を検索して入手することや、商品が例えばパーソナルコンピュータ等であった場合にソフトウェアのバージョンアップ情報の提供等が考えられる。

【0011】

このようなRFIDを利用したサービスを消費者が享受できるようにするためには、例えば、携帯電話等を利用して消費者自身が購入済商品に付されているRFIDタグをたとえば発信停止状態等にしてRFIDガード状態にし、かつ、RFID発信可能状態等のRFIDガード解除状態に切換えることができるように構成することが考えられる。しかし、消費者の操作等によってRFIDタグが発信状態（RFIDガード解除状態）あるいは発信停止状態（RFIDガード状態）に切換え可能にした場合には、発信停止状態（RF

I D ガード状態) にすべき時に消費者 (個人ユーザ) が発信停止状態 (R F I D ガード状態) にすることを忘れて怠ってしまう虞が生ずる。その場合には、前述したプライバシーの侵害問題が発生することとなる。

【 0 0 1 2 】

また、購入済商品に付されている R F I D タグを発信停止状態や発信可能状態に切換えるための操作機能を有する新たな携帯電話等の操作装置を個人ユーザが購入しない限り、そのようなモードの切換えができないのであり、モード切換え機能を有する操作装置を有しない個人ユーザの場合には、購入済商品の R F I D タグが常に R F I D 発信状態つまり、常に前述したプライバシーの侵害問題が発生する状態となるという虞がある。

【 0 0 1 3 】

さらに、今後 R F I D タグが普及してタグリーダがいたるところに設置された場合には、いたるところで前述のプライバシー問題が頻発することになるとともに、同一コードの R F I D を追跡することにより個人ユーザの移動追跡が行なわれてしまうという虞も生じる。

【 0 0 1 4 】

本発明は、係る実情に鑑み考え出されたものであり、その目的は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止することである。

【発明を解決するための手段】

【 0 0 1 5 】

請求項 1 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われ 20
るプライバシーの侵害を防止するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、

前記個人ユーザに所持されるプライバシー保護用識別子発信装置により、偽識別子を生成する偽識別子生成ステップと、

識別子の送信要求があった場合に、前記偽識別子生成ステップにより生成された前記偽識別子を前記プライバシー保護用識別子発信装置から発信する発信ステップと、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取りステップとを含み、 30

前記偽識別子生成ステップは、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成ステップを含むことを特徴とする。

【 0 0 1 6 】

請求項 2 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われ 40
るプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置を複数の個人ユーザに提供する提供ステップを含み、

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段と、

識別子の送信要求があった場合に、前記偽識別子生成手段により生成された前記偽識別 40
子を発信する発信手段とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成して発信する前記プライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持する前記プライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能であり、

前記複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に前記共通の偽識別子が異なる複数のグループに分類され、 50

前記提供ステップは、前記それぞれのグループ毎に地域を指定して該グループに属する前記プライバシー保護用識別子発信装置を個人ユーザに提供することを特徴とする。

【 0 0 1 7 】

請求項 3 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置を複数の個人ユーザに提供する提供ステップを含み

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段と、

識別子の送信要求があった場合に、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能であり、

前記提供ステップにより或る個人ユーザに提供されたプライバシー保護用識別子発信装置から、予め定められた所定個数の偽識別子を 1 度に発信し、

前記提供ステップにより前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から、前記所定個数よりも多い複数の偽識別子を 1 度に発信し、該複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成することを特徴とする。

【 0 0 1 8 】

請求項 4 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段と、

識別子の送信要求があった場合に、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段とを含むことを特徴とする。

【 0 0 1 9 】

請求項 5 に記載の本発明は、請求項 4 に記載の発明の構成に加えて、前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で前記偽識別子を生成することを特徴とする。

【 0 0 2 0 】

請求項 6 に記載の本発明は、請求項 4 または請求項 5 に記載の発明の構成に加えて、前記発信手段は、前回の偽識別子の発信から所定時間内に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信することを特徴とする。

【 0 0 2 1 】

請求項 7 に記載の本発明は、請求項 4 ～請求項 6 のいずれかに記載の発明の構成に加えて、前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能であることを特徴とする。

【 0 0 2 2 】

請求項 8 に記載の本発明は、請求項 7 に記載の発明の構成に加えて、他のプライバシー保護用識別子発信装置と交信する交信手段をさらに含み、

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段を含み、

前記交信手段は、前記他のプライバシー保護用識別子発信装置と交信して、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信

するとともに当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成することを特徴とする。

【 0 0 2 3 】

請求項 9 に記載の本発明は、請求項 8 に記載の発明の構成に加えて、前記交信手段は、互いの識別子を交換するときの交信可能通信限界距離が 20 メートル以内に定められており、該交信可能通信限界距離圏内に進入した他のプライバシー保護用識別子発信装置と交信して互いの識別子を交換することを特徴とする。

10

【 0 0 2 4 】

請求項 10 に記載の本発明は、請求項 8 または請求項 9 に記載の発明の構成に加えて、前記交信手段は、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度前記識別子の交換を行なうことを禁止する禁止手段を有することを特徴とする。

【 0 0 2 5 】

請求項 11 に記載の本発明は、請求項 8 ～請求項 10 のいずれかに記載の発明の構成に加えて、前記交信手段は、電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成することを特徴とする。

20

【 0 0 2 6 】

請求項 12 に記載の本発明は、請求項 8 ～請求項 11 のいずれかに記載の発明の構成に加えて、前記交信手段は、電子メール機能を有しており、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読出すことにより前記共通の偽識別子として生成することを特徴とする。

30

【 0 0 2 7 】

請求項 13 に記載の本発明は、請求項 4 ～請求項 12 のいずれかに記載の発明の構成に加えて、前記発信手段は、他のプライバシー保護用識別子発信装置から 1 度に発信される所定個数の偽識別子よりも多い複数の偽識別子を 1 度に発信可能であり、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成することを特徴とする。

【 0 0 2 8 】

請求項 14 に記載の本発明は、請求項 4 ～請求項 13 のいずれかに記載の発明の構成に加えて、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段と、

40

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段とを、さらに含むことを特徴とする。

【 0 0 2 9 】

請求項 15 に記載の本発明は、請求項 14 に記載の発明の構成に加えて、前記識別子ガード手段は、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にすることを特徴とする。

50

【 0 0 3 0 】

請求項 1 6 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

個人ユーザのプライバシーを保護するために匿名を名乗り匿名ユーザとして行動するために作なされた匿名と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なう登録処理ステップと、

前記匿名ユーザ用の電子証明書を発行する電子証明書発行ステップと、

前記匿名ユーザの住所を、該匿名に対応する個人ユーザとは異なった住所に設定するための住所設定ステップと、

所定の業者にユーザ登録するとき前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録ステップと、

識別子の送信要求があった場合に、前記個人ユーザに所持されるプライバシー保護用識別子発信装置から偽識別子を発信する発信ステップと、

前記ユーザ登録ステップにより前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段とを含み、

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする。

【 0 0 3 1 】

請求項 1 7 に記載の本発明は、請求項 1 6 に記載の発明の構成に加えて、前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合でないときであっても、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする。

【 0 0 3 2 】

請求項 1 8 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

個人ユーザのプライバシーを保護するために匿名を名乗り匿名ユーザとして行動するために作なされた匿名と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なう登録処理手段と、

所定の業者にユーザ登録するとき前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録手段と、

識別子の送信要求があった場合に、前記個人ユーザに所持されるプライバシー保護用識別子発信装置から偽識別子を発信する発信手段と、

前記ユーザ登録手段により前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段とを含み、

前記発信手段は、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする。

【 0 0 3 3 】

請求項 1 9 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって

所定の業者に対し個人ユーザが匿名を名乗り匿名ユーザとして行動する場合に前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段と

識別子の送信要求があった場合に偽識別子を発信する手段であって、前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する発信手段とを含むことを特徴とする

請求項 2 0 に記載の本発明は、請求項 1 9 に記載の発明の構成に加えて、前記発信手段は、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときで

あっても、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする。

【 0 0 3 4 】

請求項 2 1 に記載の本発明は、請求項 1 9 または請求項 2 0 に記載の発明の構成に加えて、前記所定の業者は、商品を販売する販売店であり、

前記匿名用偽識別子記憶手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録した当該販売店に対応する匿名用偽識別子を記憶しており、

前記発信手段は、前記販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信することを特徴とする。

【 0 0 3 5 】

請求項 2 2 に記載の本発明は、請求項 1 9 ～請求項 2 1 に記載の発明の構成に加えて、前記匿名用偽識別子記憶手段は、複数の前記業者に対応してそれぞれ異なった匿名用偽識別子を記憶しており、

前記発信手段は、前記複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から選択して発信することを特徴とする。

【 0 0 3 6 】

請求項 2 3 に記載の本発明は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプログラムであって、

プライバシー保護用識別子発信装置に設けられているコンピュータに、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型。偽識別子生成手段と、

識別子の送信要求があった場合に、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段と、

して機能させる。

【 0 0 3 7 】

請求項 2 4 に記載の本発明は、請求項 2 3 に記載の発明の構成に加えて、前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で前記偽識別子を生成させることを特徴とする

請求項 2 5 に記載の本発明は、請求項 2 3 または請求項 2 4 に記載の発明の構成に加えて、前記発信手段は、前回の偽識別子の発信から所定時間内に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信させることを特徴とする。

【 0 0 3 8 】

請求項 2 6 に記載の本発明は、請求項 2 3 ～請求項 2 5 のいずれかに記載の発明の構成に加えて、前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能にすることを特徴とする。

【 0 0 3 9 】

請求項 2 7 に記載の本発明は、前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段を含み、

前記他のプライバシー保護用識別子発信装置と交信して、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信させるとともに当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手

段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させることを特徴とする。

【0040】

請求項28に記載の本発明は、請求項26または請求項27に記載の発明の構成に加えて、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度前記識別子の交換を行なうことを禁止する禁止手段として機能させることを特徴とする。

【0041】

請求項29に記載の本発明は、請求項26～請求項28のいずれかに記載の発明の構成に加えて、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させることを特徴とする。

【0042】

請求項30に記載の本発明は、請求項26～請求項29のいずれかに記載の発明の構成に加えて、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読み出すことにより前記共通の偽識別子として生成させることを特徴とする。

【0043】

請求項31に記載の本発明は、請求項23～請求項30のいずれかに記載の発明の構成に加えて、前記発信手段は、他のプライバシー保護用識別子発信装置から1度に発信される所定個数の偽識別子よりも多い複数の偽識別子を1度に発信させることが可能であり、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成させることを特徴とする。

【0044】

請求項32に記載の本発明は、請求項23～請求項31のいずれかに記載の発明の構成に加えて、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段と、

して機能させるプログラムをさらに含むことを特徴とする

請求項33に記載の本発明は、請求項32に記載の発明の構成に加えて、前記識別子ガード手段は、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にさせることを特徴とする。

【発明の効果】

【0045】

請求項1に記載の本発明によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を個人ユーザの意思に従って読取ることができるように

するために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要な時に読取ってサービス等を楽しむことが可能となる。

【 0 0 4 6 】

また、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【 0 0 4 7 】

請求項 2 に記載の本発明によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【 0 0 4 8 】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【 0 0 4 9 】

さらに、複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に共通の偽識別子が異なる複数のグループに分類されており、それぞれのグループ毎に地域を指定してそのグループに属するプライバシー保護用識別子発信装置が個人ユーザに提供される。その結果、各地域内の者同士で共通の偽識別子を生成して発信する傾向が生じ、前述の異人物同一識別子発信現象を極力各地域内の個人ユーザ同士で生じさせることができ、悪意のプライバシー侵害者に対する前述した攪乱効果をより効果的に発揮することができる。

【 0 0 5 0 】

請求項 3 に記載の本発明によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異

なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【 0 0 5 1 】

10

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【 0 0 5 2 】

また、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が一度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前述の所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信される。その結果、個人ユーザに携帯された購入済物品に付されている無線識別子発信装置が常時識別子が発信される状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 5 3 】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有の識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【 0 0 5 4 】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前述の所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と携帯している購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザから発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複

50

数箇所では識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【 0 0 5 5 】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物間で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

【 0 0 5 6 】

請求項 4 に記載の本発明によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【 0 0 5 7 】

請求項 5 に記載の本発明によれば、請求項 4 に記載の発明の効果に加えて、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

【 0 0 5 8 】

請求項 6 に記載の本発明によれば、請求項 4 または請求項 5 に記載の発明の効果に加えて、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

【 0 0 5 9 】

請求項 7 に記載の本発明によれば、請求項 4 ～請求項 6 のいずれかに記載の発明の効果に加えて、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信

頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【 0 0 6 0 】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

10

【 0 0 6 1 】

請求項 8 に記載の発明の効果は、請求項 7 に記載の発明の効果に加えて、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別子を交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 6 2 】

20

請求項 9 に記載の本発明によれば、請求項 8 に記載の発明の効果に加えて、互いの識別子を交換するときの交信可能通信限界距離が 20 メートル以内に定められており、その交信可能通信限界距離圏内に進入したプライバシー保護用識別子発信装置と互いに交信して識別子が交換されるために、20 メートル以内という比較的近距离圏内に位置する個人ユーザの間で互いの識別子の交換がなされることとなり、比較的近くに位置していた者同士で共通の偽識別子を共有して発信できる状態となり、前述の異人物同一識別子発信現象を極力近距离圏内に位置していた個人ユーザ同士で生じさせることができ、悪意のプライバシー侵害者に対する前述した攪乱効果をより効果的に発揮することができる。

【 0 0 6 3 】

請求項 10 に記載の本発明によれば、請求項 8 または請求項 9 に記載の効果に加えて、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

30

【 0 0 6 4 】

請求項 11 に記載の本発明によれば、請求項 8 ～請求項 10 のいずれかに記載の発明の効果に加えて、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 6 5 】

請求項 12 に記載の本発明によれば、請求項 8 ～請求項 11 に記載の発明の効果に加えて、交信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

40

【 0 0 6 6 】

請求項 13 に記載の本発明によれば、請求項 4 ～請求項 12 の何れかに記載の発明の効果に加えて、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が 1 度に発信される一方、前記或る個人ユーザとは異なる他

50

の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 6 7 】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【 0 0 6 8 】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【 0 0 6 9 】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

【 0 0 7 0 】

請求項 1 4 に記載の本発明によれば、請求項 4 ～請求項 1 3 のいずれかに記載の発明の効果に加えて、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を個人ユーザの意思に従って読取ることができるようにするために、購入済み

の物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要なときに読取ってサービス等を享受することが可能となる。

【 0 0 7 1 】

請求項 1 5 に記載の本発明によれば、請求項 1 4 に記載の発明の効果に加えて、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

10

【 0 0 7 2 】

請求項 1 6 に記載の本発明によれば、個人ユーザのプライバシーを保護するために匿名を作成しその匿名を名乗って行動する匿名ユーザ用の電子証明書が発行されるため、匿名ユーザでありながらも発行された電子証明書を提示することにより売買等の取引行為の主体になることが可能となる。しかも、匿名ユーザの住所が、該匿名に対応する個人ユーザとは異なった住所に設定されているために、住所を手がかりにどの個人ユーザがどの匿名ユーザに該当するのかを見破られてしまう不都合も極力防止できる。また、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらも該業社に対し売買等の取引行為を行なうことができるとともに、ユーザ登録によるサービス等を享受することができる。

20

【 0 0 7 3 】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子とその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより業社側は、たとえば、移動する匿名ユーザから発せられる識別情報を要所所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

30

【 0 0 7 4 】

請求項 1 7 に記載の本発明によれば、請求項 1 6 に記載の発明の効果に加えて、匿名を登録している業者に対し偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、その匿名をユーザ登録している業社からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報の横流しを監視することが可能となる。

40

【 0 0 7 5 】

請求項 1 8 に記載の本発明によれば、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらもユーザ登録によるサービス等を享受することができる。

【 0 0 7 6 】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザ

50

から発信された識別子はその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【 0 0 7 7 】

請求項 19 に記載の本発明によれば、所定の業者に対し個人ユーザが匿名を名乗り匿名ユーザとして行動する場合に前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、識別子の送信要求があった場合に、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信する。業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子とその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【 0 0 7 8 】

請求項 20 に記載の本発明によれば、請求項 19 に記載の発明の効果に加えて、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、個人ユーザが匿名を名乗る前記業者からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報情報の横流しを監視することが可能となる。

【 0 0 7 9 】

請求項 21 に記載の本発明によれば、請求項 19 または請求項 20 に記載の発明の効果に加えて、販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録することにより、当該販売店において匿名ユーザとして行動して商品購入等を行なうことができ、個人ユーザのプライバシーを保護しながらもポイント付与のサービスも享受できる。また、販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に、無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、匿名用偽識別子が匿名用偽識別子記憶手段から読出されて発信されるために、自動決済を行なうことができながらも、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【 0 0 8 0 】

請求項 2 2 に記載の本発明によれば、請求項 1 9 ～請求項 2 1 に記載の発明の効果に加えて、匿名用偽識別子記憶手段は、複数の前記業者に対応してそれぞれ異なった匿名用偽識別子を記憶しており、発信手段は、複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から選択して発信するために、業社毎に異なった匿名用識別子を使分けることができる。

【 0 0 8 1 】

請求項 2 3 に記載の本発明によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【 0 0 8 2 】

請求項 2 4 に記載の本発明によれば、請求項 2 3 に記載の発明の効果に加えて、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

【 0 0 8 3 】

請求項 2 5 に記載の本発明によれば、請求項 2 3 または請求項 2 4 に記載の発明の効果に加えて、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

【 0 0 8 4 】

請求項 2 6 に記載の本発明によれば、請求項 2 3 ～請求項 2 5 のいずれかに記載の発明の効果に加えて、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報等を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【 0 0 8 5 】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユ

一ザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという攪乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【 0 0 8 6 】

請求項 2 7 に記載の発明の効果は、請求項 2 6 に記載の発明の効果に加えて、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別子を交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 8 7 】

請求項 2 8 に記載の本発明によれば、請求項 2 6 または請求項 2 7 に記載の効果に加えて、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

【 0 0 8 8 】

請求項 2 9 に記載の本発明によれば、請求項 2 6 ～請求項 2 8 のいずれかに記載の効果に加えて、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 8 9 】

請求項 3 0 に記載の本発明によれば、請求項 2 6 ～請求項 2 9 に記載の発明の効果に加えて、交信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 9 0 】

請求項 3 1 に記載の本発明によれば、請求項 2 3 ～請求項 3 0 の何れかに記載の発明の効果に加えて、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が 1 度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【 0 0 9 1 】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、1 度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所では識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。そ

の結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【 0 0 9 2 】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所でも識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【 0 0 9 3 】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ

請求項 3 2 に記載の本発明によれば、請求項 2 3 ～請求項 3 1 のいずれかに記載の発明の効果に加えて、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービスを個人ユーザが受けたいと思う必要なときに読取ってサービスを楽しむことが可能となる。

【 0 0 9 4 】

請求項 3 3 に記載の本発明によれば、請求項 3 2 に記載の発明の効果に加えて、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

【 発明を実施するための最良の形態 】

【 0 0 9 5 】

次に、本発明の実施の形態を図面に基いて詳細に説明する。図 1 は、ブロードバンドを利用したネットワークシステム全体の概略を示す構成図である。広域・大容量中継網 4 3 を通じて、クレジットカード発行会社群 4、加盟店契約会社群 5、受信局 4 2、加盟店群 6、サプライヤ群 S、NM 群（ニューミドルマン群） 4 8、電子行政群 4 9、X M L ス

トア 5 0、コンテンツプロバイダ群 5 1、信号 5 2、携帯電話網 5 4 に接続されたゲートウェイ 5 3、インターネット I、ユーザ宅 4 7、認証局群 4 6、コンビニエンスストア群 2、会社群 4 5、データセンタ 4 4、ライフ支援センタ 8、放送局 4 1、金融機関群 7 等が、情報の送受信ができるように構成されている。なお、図中 4 0 は衛星（サテライト）であり、放送局 4 1 からの放送電波を中継して受信局 4 2 に電波を送るためのものである。

【 0 0 9 6 】

クレジットカード発行会社群 4 とは、たとえば S E T (Secure Electronic Transaction) により決済を行なう場合のイシュアとしての機能を発揮するカード発行会社である。加盟店契約会社群 5 は、電子モール等を構成する加盟店群 6 が契約している金融機関等からなる会社であり、S E T におけるアクアイアラとして機能する機関である。サプライヤ群 S とは、商品メーカー等であり、商品や情報を提供する機関のことである。N M 群 4 8 とは、サプライヤ群 S と消費者（自然人または法人）との仲立ちを行ない、たとえば消費者のショッピング等の消費行動の支援を行なうサービス業者のことである。従来の問屋や商社等の中間業者が、サプライヤ群の販売支援を行なうのに対し、この N M 群 4 8 は、消費者の購入支援（消費行動支援）を行なう点で相違する。N M 群 4 8 の具体例としては、消費者の嗜好情報や購買履歴情報や W e b サイトへのアクセス履歴情報をデータベースとして蓄積し、その蓄積されている消費者のプロフィール情報（個人情報）に基づいてその消費者にマッチする商品情報等を推薦して、消費者の消費行動を助けるサービス業者が当てはまる。

20

【 0 0 9 7 】

電子行政群 4 9 は、たとえば市役所や税務署あるいは中央官庁等の行政を電子化したものである。X M L ストア 5 0 とは、X M L による統一されたデータ構造によってデータを格納するとともに、必要に応じてデータの要求者に所定のデータを提供するデータベースのことである。X M L ストア 5 0 には、ユーザの各種個人情報やユーザエージェント（エージェント用知識データを含む）を格納している。金融機関群 7 やユーザから X M L ストア 5 0 にアクセスがあった場合には、本人認証を行なってセキュリティを保ったうえで、必要なデータを提供できるように構成されている。コンテンツプロバイダ群 5 1 とは、映像、文字、音等の種々のコンテンツをネットワークを通じて提供する業者群のことである。交通整理を行なうための信号機 5 2 も、広域・大容量中継網 4 3 に接続され、遠隔制御できるように構成されている。

30

【 0 0 9 8 】

携帯電話網 4 5 に接続されている基地局 5 5 に対し、ブラウザフォン（携帯電話） 3 0 の電波が送信され、基地局 5 5、携帯電話網 4 5、ゲートウェイ 5 3、広域・大容量中継網 4 3 を介して、金融機関群 7、加盟店群 6、N M 群 4 8、電子行政群 4 9、X M L ストア 5 0、コンテンツプロバイダ群 5 1 等にアクセスできるように構成されている。また車両 5 6 も同様に、基地局 5 5、携帯電話網 5 4、ゲートウェイ 5 3、広域・大容量中継網 5 4 を介して、各種サービス業者や各種機関にアクセスできるように構成されている。

【 0 0 9 9 】

認証局群 4 6 とは、電子証明書の発行希望者に対して本人認証をしたうえで電子証明書 40 を発行する機関である。データセンタ 4 4 は、放送局 4 1 から電波により配信される各種データを格納、管理する機関のことである。加盟店群 6、サプライヤ群 S、N M 群 4 8、電子行政群 4 9、コンテンツプロバイダ群 5 1 等にユーザが所定の情報の送信を依頼した場合に、大容量のデータを送信する際には、それら各機関やサービス業者の配信するデータを一旦データセンタ 4 4 に格納しておき、所定の日時が来たときに放送局 4 1 から電波を通じてそのデータを配信し、受信局 4 2 で受信したデータを所定のユーザに広域・大容量中継網 4 3 を通じて配信する。

【 0 1 0 0 】

8 はライフ支援センターである。このライフ支援センター 8 は、ユーザの個人情報を収集し、その個人情報に基づきユーザにふさわしい夢、人生設計、職種、趣味等を推薦して 50

、それらを実現するために必要となる各種商品や情報を提供してくれる加盟店（ニューミドルマンを含む）を推薦するサービスを行なう機関である。

【 0 1 0 1 】

なお、図 1 中二重線で示した部分は、無線 LAN, CATV, 衛星, xDSL (digital subscriber line), FTTN (fiber to the home) などである。

【 0 1 0 2 】

本実施の形態では、認証局群 4 6 ばかりでなく、金融機関群 7 も、電子証明書を発行する。図 1 中、19 はユーザに携帯される IC 端末であり、後述するようにユーザのプロファイル情報（個人情報）等が格納されている。

【 0 1 0 3 】

図 2 は、金融機関 7 を説明するための説明図である。金融機関 7 には、VP 管理サーバ 9、決済サーバ 10、認証用サーバ 11、データベース 12a, 12b が備えられている。VP 管理サーバ 9 は、仮想人物としてのバーチャルパーソン（以下、単に「VP」という）を管理するためのサーバである。VP とは、現実世界に実在しないネットワーク上等で行動する仮想の人物のことであり、現実世界での実在人物であるリアルパーソン（以下、単に「RP」という）がネットワーク上等で行動する際に、VP になりすましてその VP として行動できるようにするために誕生させた仮想人物のことである。また、後述するように、RP が、ネットワーク上で行動するときばかりでなく、現実世界で行動するときにも VP になりすましてその VP として行動する場合がある。

【 0 1 0 4 】

VP 管理サーバ 9 は、後述するように、RP から VP の出生依頼があれば、その VP の氏名や住所等の所定情報を決定して VP を誕生させ、その VP のデータをデータベース 12a に記憶させておく機能を有している。また、この VP 管理サーバ 9 は、VP 用の電子証明書を作成して発行する機能も有している。VP が売買や決済等の法律行為を行なう場合に、この電子証明書を相手方に送信することにより、仮想人物でありながら独立して法律行為を行なうことが可能となる。

【 0 1 0 5 】

認証用サーバ 11 は、RP 用の電子証明書を作成して発行する機能を有する。金融機関 7 に設置されている決済サーバ 10 は、RP による電子マネーやデビットカードを使用しての決済ばかりでなく、VP として電子マネーやデビットカードを使用しての決済を行なうための処理を行なう機能も有している。

【 0 1 0 6 】

データベース 12a は、RP や VP に関するデータを格納するものである。データベース 12b は、広域・大容量中継網 43 やインターネット I に接続されているサイト（業者）を管理するためのデータを格納している。

【 0 1 0 7 】

図 2 に示すように、データベース 12a には、RP 用のデータとして、RP の氏名、住所、認証鍵 KN、公開鍵 KT、口座番号等が記憶されている。認証鍵とは、RP が金融機関 7 にアクセスしてきた場合に共通鍵暗号方式により本人認証を行なうための鍵である。公開鍵とは、公開鍵暗号方式に用いられる鍵であり、秘密鍵とペアとなっている鍵である。口座番号は、当該金融機関 7 において RP が開設している口座番号のことである。

【 0 1 0 8 】

トラップ情報とは、サイト（業者）側が個人情報を収集してそれを不正に流通させた場合に、それを行なった犯人を割出すためにトラップ（罠）を仕掛けるための情報である。たとえば、VP が自己の個人情報のある業者（第 1 譲渡先）に譲渡する際に、その第 1 譲渡先特有の氏名を用いる。すなわち、VP が自己の氏名を複数種類有し、サイト（業者）ごとに使い分ける。このような VP 氏名を、便宜上トラップ型 VP 氏名という。このようにすれば、ダイレクトメールや E メールが業者側から送られてきた場合には、そのメールの宛名がトラップ型 VP 氏名となっているはずである。その送ってきたサイト（業者）が、トラップ型 VP 氏名から割出される第 1 譲渡先とは異なりかつ譲渡した自己の個人情報

の開示許容範囲（流通許容範囲）を超えたサイト（業者）であった場合には、その個人情報が第1譲渡先によって不正に開示（流通）されたこととなる。このように、不正流通（不正開示）を行なった第1譲渡先を、トラップ型VP氏名から割出すことができる。

【0109】

なお、図2では、次郎が第2トラップ情報、第3トラップ情報、第2個人情報、第3個人情報、2つの情報を有している。次郎が、ネットワーク上で行動する場合に、この2人のVPを使い分けて行動するために、これら2種類のVP情報を金融機関7に登録している。VPの住所とは、後述するように、RPの希望するまたはRPの住所に近いコンビニエンスストア2の住所である。その結果、VPとして電子ショッピングをした場合の商品の配達先が、そのVPの住所であるコンビニエンスストア2に配達されることとなる。RPは、その配達されてきた商品をVPになりすましてコンビニエンスストア2にまで出向いて商品を引取ることが可能となる。このようにすれば、住所を手がかりにVPとRPとの対応関係が見破られてしまう不都合が防止できる。

【0110】

図2に示したトラップ情報の詳細は、図3に示されている。第1トラップ情報、第2トラップ情報、…の各トラップ情報は、サイト名（業社名）ごとに、氏名（トラップ型VP氏名）、公開鍵、Eメールアドレス、バーチャル口座番号、バーチャルクレジット番号を含んでいる。たとえば、サイト名（業者名）ABCにVPがアクセスする際には、VPの本名であるB13Pを用い、VPの秘密鍵KSBとペアの公開鍵KP B'を用い、VPの本当のEメールアドレスである○□×△×を用い、VPの本当の口座番号である2503を用い、VPの本当のクレジット番号である3288を用いる。

【0111】

一方、サイト名（業者名）MTTにアクセスする（MTTで図30の自動決済を行う）場合には、VPの本名をそのVPの秘密鍵で1回暗号化したE（B13P）を、トラップ型VP氏名として用いる。秘密鍵としては、VPの本当の秘密鍵KSBをVPの本当の秘密鍵KSBで1回暗号化したEKS B（KSB）を用いる。この秘密鍵EKS B（KSB）に対する公開鍵KP Bがデータベース12aに格納されている。Eメールアドレスとしては、金融機関7がトラップ型VPのために開設しているEメールアドレス△△△△△を用いる。口座番号としては、VPの本当の口座番号をVPの本当の秘密鍵で1回暗号化したE（2503）をバーチャル口座番号として用いる。クレジット番号は、VPの本当のクレジット番号をVPの本当の秘密鍵で1回暗号化したE（3288）を用いる。

【0112】

さらに、サイト名（業者名）MECにアクセスする（MECで図30の自動決済を行う）場合には、VPの秘密鍵でVPの本名を2回暗号化したE2（B13P）をトラップ型VP氏名として用いる。

【0113】

VPがトラップ型VP氏名E2（B13P）を用いてネットワーク上で行動する場合には、秘密鍵KSBを秘密鍵KSBで2回暗号化した2回暗号化秘密鍵E2KS B（KS B）を用いる。その2回暗号化秘密鍵とペアになっている公開鍵がKP B''である。Eメールアドレスは、金融機関7がトラップ型VP用のEメールアドレスとして開設している△△△△△を用いる。バーチャル口座番号は、VPの本当の口座番号を秘密鍵で2回暗号化したE2（2503）を用いる。クレジット番号は、VPの本当のクレジット番号をVPの秘密鍵で2回暗号化したバーチャルクレジット番号E2（3288）を用いる。

【0114】

このように、サイト名（業社名）ごとに、トラップ情報の暗号回数が異なる。サイト側（業者側）に提供した個人情報というものは、ネットワーク上を流通した後最終的にはその個人情報主にEメールやダイレクトメールの形で返ってくる。この個人情報の帰還ループを利用してトラップを仕掛けて個人情報の不正流通を行なった犯人を追跡できるようにするのが、このトラップ情報の狙いである。すなわち、ユーザをネット上で追跡するトラッキング型クッキーの逆を行なうものである。

【 0 1 1 5 】

図 4 は、図 2 に示した V P の個人情報 を説明する図である。第 1 個人情報、第 2 個人情報、第 3 個人情報、…の各個人情報は、個人情報 A、個人情報 B、…の複数種類の個人情報が集まって構成されている。たとえば、個人情報 A は、V P の年齢、性別、職業、年収等であり、個人情報 B は、V P の嗜好に関する情報である。

【 0 1 1 6 】

図 4 に示すように、各個人情報は、金融機関 7 の秘密鍵 K S によるデジタル署名が付されている。たとえば、第 1 個人情報の個人情報 A は、〇〇△の個人情報自体に対しデジタル署名である D_{KS} (〇〇△) が付されている。

【 0 1 1 7 】

このデータベース 1 2 a に格納されている各個人情報は、後述するように、金融機関 7 がその真偽をチェックして正しいもののみをデータベース 1 2 a に格納し、正しいことを認証するためのデジタル署名が付される。

【 0 1 1 8 】

図 5 は、XML ストア 5 0 の構成を示す図である。XML ストア 5 0 には、データベース 7 2 とそれを制御するサーバ 7 1 とが設置されている。サーバ 7 1 は、XML ストア 5 0 にアクセスしてきた者を、本人認証してアクセス制御する機能も備えている。

【 0 1 1 9 】

データベース 7 2 には、XML で表現されたデータが格納されている。そのデータの中身は、V P 情報として、V P の氏名であるたとえば B 1 3 P、V P ユーザエージェント (20 知識データを含む)、サイト (業社) 別情報として、サイト名 (業社名) たとえば A B C、そのサイト (業社) にアクセスした V P に発行された電子証明書、その V P の個人情報と当該サイト (業社) のプライバシーポリシーとそれら両情報に対し当該 V P が付したデジタル署名 D_{KSB} (個人情報 + ポリシー) と当該サイト (業社) A B C が付したデジタル署名 D_{KSA} (個人情報 + ポリシー) と、トラップ情報としての暗号化回数「0」と、当該 V P の E メールアドレスである $\square \times \triangle \times$ が含まれている。さらに、V P がサイト名 (業社名) M T T にアクセスした場合には、そのサイト名 (業社名) M T T にアクセスしたトラップ型 V P に対し発行された電子証明書と、そのサイト (業社) にトラップ型 V P が提供した個人情報とそのサイト (業社) のプライバシーポリシーとそれら両情報に対する当該トラップ型 V P のデジタル署名と当該サイト (業社) のデジタル署名と、トラップ 30 情報としての暗号回数「1」と E メールアドレスとが含まれている。

【 0 1 2 0 】

さらに、氏名が N P X A の他の V P の情報も、前述と同様の項目がデータベース 7 2 に記憶される。このデータベース 7 2 には、非常に多くの V P ごとに、前述した項目でデータが記憶されている。

【 0 1 2 1 】

なお、サイト名 (業社名) A B C については、図 3 で説明したように、トラップ情報として 1 回も暗号化していない情報を用いているために、データベース 7 2 に格納されている暗号回数も「0」となっている。サイト名 (業社名) M T T について言えば、図 3 で説明したように、トラップ情報として 1 回暗号化した情報を用いているために、データベ 40 ス 7 2 に記憶されている暗号化回数も「1」となっている。

【 0 1 2 2 】

前述した V P ユーザエージェントとは、ユーザである V P のために動作する自立型ソフトウェアのことである。この V P ユーザエージェントは、ネットワークを通して移動できるようにモバイルエージェントで構成されている。

【 0 1 2 3 】

なお、図 2 ～図 5 に示した各データは、暗号化した状態で各データベースに格納しておいてもよい。そうすれば、万一データが盗まれたとしても、解読できないために、セキュリティ上の信頼性が向上する。一方、たとえば V P (トラップ型 V P を含む) がネットワーク上で目に余る不正行為 (たとえば刑法に違反する行為) を行なった場合には、所定機 50

関（たとえば警察等）からの要請等に応じて、そのVPをデータベース12a等から検索してそのVPに対応するRPを割出し、RPの住所氏名等を要請のあった所定機関（たとえば警察等）に提供するようにしてもよい。

【0124】

図6は、コンビニエンスストア2の構成を示す図である。コンビニエンスストア2には、データベース75と、それに接続されたサーバ74と、そのサーバに接続された端末73とが設置されている。データベース75には、当該コンビニエンスストアに住所を持つVP（トラップ型VPを含む）の氏名と、それら各氏名に対応して、商品の預かり情報、Eメールアドレス、顧客管理情報等が記憶されている。

【0125】

当該コンビニエンスストア2にB13PのVPが購入した商品が配達されれば、データベース75のB13Pの記憶領域に、商品預かり情報として「ABC会社からの商品預かり、未決済」が格納される。この未決済とは、B13Pがネットを通じて商品を購入したもののまだ支払を行っていない状態のことである。

【0126】

データベース75のEメールアドレスの欄には、各VPに対応してEメールアドレスが格納されている。B13Pの場合には、トラップ型VPでないために、当該VPの本当のEメールアドレスである○□×△×が格納されている。

【0127】

トラップ型VPであるE（B13P）も同様に、商品預かり情報としてたとえば「MT 20 T会社からの商品預かり、決済済」が格納される。なお、E（B13P）は、トラップ型VPであるために、Eメールアドレスは、金融機関7のトラップ型VPのために開設されているEメールアドレスが格納される。

【0128】

サーバ74は、後述するように、コンビニエンスストア2にVP（トラップ型VPを含む）として商品を引取りに来た顧客が、当該コンビニエンスストア2に登録されているVP（トラップ型VPを含む）に対し商品を預かっている場合にはその商品をVP（トラップ型VPを含む）に引渡すための処理を行なう。

【0129】

コンビニエンスストア2は、商品の預かりサービスばかりでなくVP用のダイレクトメールの預かりサービスも行なう。VPはコンビニエンスストア2が住所でありVP宛のダイレクトメールはコンビニエンスストア2に郵送されるためである。

【0130】

図7は、ユーザに用いられる端末の一例のブラウザフォン30を示す正面図である。ブラウザフォン30には、マイクロコンピュータ199が備えられている。このマイクロコンピュータ199には、CPU（Central Processing Unit）197と、I/Oポート198と、ROM195と、EEPROM194と、RAM196とが備えられている。このブラウザフォン30は、USB（Universal Serial Bus）ポートを備えており、USB 30 ポートに対し、IC端末19Rまたは19Vまたは19Iが差込み可能に構成されている。IC端末19Rは、RP用のIC端末である。IC端末19Vは、VP用のIC端末である。IC端末19Iは、後述するように金融機関が発行したVP用のデータやプログラムが格納されてユーザにまで配達されてくるものであり、その配達されてきたIC端末19Iをブラウザフォン30のUSBポートに指込むことにより、IC端末19Iに記憶されているデータやソフトウェアがブラウザフォン30に記憶されることとなる。なお、各IC端末19R、19V、19Iは、ICカードで構成してもよい。

【0131】

図8は、VP用IC端末19Vを説明するための説明図である。VP用IC端末19Vは、前述したように、ブラウザフォン30のUSBポート18に対し着脱自在に構成されており、USBポート18に差込むことにより、ブラウザフォン30との情報がやり取りできるようになり、使用可能な状態となる。

【 0 1 3 2 】

VP用IC端末19V内には、LSIチップ20が組込まれている。このLSIチップ20には、制御中枢としてのCPU24、CPU24の動作プログラムが記憶されているROM25、CPU24のワークエリアとしてのRAM22、電氣的に記憶データを消去可能なEEPROM26、コプロセッサ23、外部とのデータの入出力を行なうためのI/Oポート21等が設けられており、それらがバスにより接続されている。

【 0 1 3 3 】

EEPROM26には、電子マネー用のプログラムであるモンデックス（リロード金額データを含む）、その他の各種アプリケーションソフト、VP用に発行された電子証明書、暗証番号、トラップ型RFIDが記憶されている。このトラップ型RFIDとは、ユーザがトラップ型VPとして行動する際にそのトラップ型VPに対応するRFIDを発信するために記憶しているRFIDである。詳しくは後述する。 10

【 0 1 3 4 】

さらに、VP用IC端末19Vは、VPのユーザエージェントとしての機能を有しており、ユーザエージェント用知識データとして、デビットカード情報、クレジットカード情報、VPの氏名、住所、VPのEメールアドレス、VPの公開鍵KPと秘密鍵KS、RPの認証鍵KN、VPの年齢、職業等、VPの各種嗜好情報、VPの家族構成、…等の各種知識データが記憶されている。

【 0 1 3 5 】

RP用IC端末19Rの場合も、図8に示したVP用IC端末19Vとほぼ同様の構成を有している。相違点といえば、EEPROM26に記録されているユーザエージェント用知識データの内容が相違する。具体的には、VPの氏名、住所の代わりにRPの氏名、住所、VPのEメールアドレスの代わりにRPのEメールアドレス、VPの公開鍵や秘密鍵の代わりにRPの公開鍵、秘密鍵、VPの年齢や職業等の代わりにRPの年齢や職業等、VPの各種嗜好情報の代わりにRPの各種嗜好情報、VPの家族構成の代わりにRPの家族構成となる。トラップ型RFIDは記憶していない。 20

【 0 1 3 6 】

なお、VPの家族構成は、VPに対応するRPの家族がVPを誕生させている場合には、その誕生しているVPの名前や住所や年齢等のデータから構成されている。つまり、RPの家族に対応するVPの家族すなわちバーチャル家族のデータがこのVPの家族構成の記憶領域に記憶されることとなる。 30

【 0 1 3 7 】

図9は、図8に示したトラップ型RFIDの詳細を示す図である。トラップ型RFIDの記憶領域には、VP氏名ごとに、そのVP氏名に対応するトラップ型RFIDが格納される。たとえば量販店等の業社NTTでVPとしてポイントカード等を作成する際にVPがトラップ型VP名E（B13P）を登録した場合には、その業社でショッピング等の行動を行なう際にE（B13P）に対応するトラップ型RFIDであるmttをブラウザフォン（携帯電話）30から発信する。そのために各トラップ型VPに対応させてトラップ型RFIDを記憶させている。たとえば、業社MTT内でショッピング等の行動を行なう際にE（B13P）に対応するトラップ型RFIDであるmttをブラウザフォン（携帯電話）30から発信し、トラップ型VP名E²（B13P）を登録している業社MEC内でショッピング等の行動を行なう際同じmttをブラウザフォン（携帯電話）30から発信した場合には、RFIDmttを手がかりにE（B13P）とE²（B13P）とは同一人物であることが見破られてしまう虞がある。このような不都合を防止するために、業社毎に発信するRFIDを異ならせる。 40

【 0 1 3 8 】

また、たとえば業社MTT内でショッピング等の行動を行なう際にE（B13P）に対応するトラップ型RFIDであるmttをブラウザフォン（携帯電話）30から発信し、かつ、VP名等の個人情報的一切登録していない小売店AMPMでショッピング等の行動をする際にmttを発信し、後日小売店AMPMから電子メールまたはダイレクトメール 50

がE (B 1 3 P)宛に送られてきた場合には、E (B 1 3 P)の個人情報 が業社M T Tから小売店A M P Mに不正に横流しされたことになる。そのような横流しを監視することができる。

【 0 1 3 9 】

なお、I C 端末1 9 V, 1 9 RのE E P R O M 2 6には、公開鍵K P、秘密鍵K S、認証鍵K N、暗証番号のみを記憶させ、それ以外の情報はすべてX M Lストア5 0の方に記憶させて必要に応じて検索して利用できるようにしてもよい。また、公開鍵K P、秘密鍵K Sを用いた暗号化や復号処理は、I C 端末1 9 V, 1 9 R自体が行うのではなく、ブラウザフォン3 0あるいは後述するパーソナルコンピュータ3 0'が行うようにしてもよい。その場合には、公開鍵K P、秘密鍵K Sをブラウザフォン3 0あるいは後述するパーソナルコンピュータ3 0'に出力する必要がある。

【 0 1 4 0 】

図1 0は、携帯装置1の機能の概略を示すブロック図である。図4を参照して、携帯装置1は、たとえば指輪の形状をしており、ユーザの身体に装着しやすい形状となっている。以下、携帯装置1をI Dリング1という。I Dリング1は、入浴や就眠時も常時身につけることを原則とし、このことにより紛失や盗難を防ぐことができる。また、I Dリング1にはセキュリティ用のR F I Dタグ1 aが設けられており、そのR F I Dタグ1 aは、R F I Dタグ1 aの全体を制御するためのロジック (C P U) 1 0 0と、暗号化されたR F I Dを記憶するための読出し専用メモリ (R O M : Read Only Memory) 1 0 1と、ロジック1 0 0で実行する際に必要なランダムアクセスメモリ (R A M : Random Access Memory) 1 0 2と、電気消去可能プログラマブル読出し専用メモリ (E E P R O M : electrically erasable programmable read-only memory) 1 0 3と、電源に用いられる電波を受信し、信号を送受信するためのループアンテナ1 0 7 a、1 0 7 bと、受信された電源に用いられる電波から電力を発生するための電源制御部1 0 6と、受信した信号を復調し、送信するための信号を変調するための変調・復調部1 0 5と、変調・復調部1 0 5への信号の入出力を制御するための入出力制御部1 0 4とを含む。ロジック1 0 0、R O M 1 0 1、R A M 1 0 2、E E P R O M 1 0 3、入出力制御部1 0 4は、それぞれデータバス1 0 8によって接続されている。

【 0 1 4 1 】

ロジック1 0 0は、R O M 1 0 1、R A M 1 0 2、E E P R O M 1 0 3、入出力制御部1 0 4を制御して、後述する各種処理を実行する。

【 0 1 4 2 】

R O M 1 0 1は、R F I Dタグ1 aに付され、他のR F I Dタグ1 aと識別するためのR F I Dとを記憶する。R F I Dは、R F I Dタグ1 aが製造される段階、または、ユーザに発行される前の段階で記録され、その後消去されることはない。

【 0 1 4 3 】

E E P R O M 1 0 3には、ブラウザフォン3 0から送信されてきた本人認証用のパスワードが記憶される。後述するようにR F I Dタグ1 aを一旦発信停止状態にした後発信を再開できる状態にするとときに、ブラウザフォン3 0からパスワードが送信され、その送信されてきたパスワードを予めE E P R O M 1 0 3に記憶されているパスワードと照合し一致すると判断された場合にのみ、R F I Dタグ1 aがR F I Dを発信できる状態に切換わる。

【 0 1 4 4 】

入出力制御部1 0 4は、C P U 1 0 0により制御され、変調・復調部1 0 5およびループアンテナ1 0 7 aを介して情報を送受信する。これにより、R F I Dタグ1 aは、スキャナ (R F I Dタグリーダライタ) 2 0 1と無線による通信が可能である。R F I Dタグ1 aとスキャナ2 0 1との間の通信は、非接触型のI Cカードを用いた場合の通信と同様の技術が用いられる。したがって、ここではその詳細な説明は繰返さない。

【 0 1 4 5 】

一方のループアンテナ1 0 7 bには大容量のコンデンサ1 1 0が接続されており、電源

に用いられる電波をこのループアンテナ107bが受信してコンデンサ110に電力を貯えるように構成されている。電源に用いられる電波の送信が停止したときにこのコンデンサ110に貯えられている電力を電源制御部106に供給して引き続き所定時間（たとえば10秒程度）RFIDタグ1aが作動できるように構成されている。

【0146】

図11は、図10に示したRFIDタグ1aのロジック(CPU)100の制御動作を示すフローチャートである。まずSA1により、RFID送信指令を受信したか否かの判断がなされ、受信するまで待機する。タグリーダから電源用の電波が発せられて静電誘導によりループアンテナ107aに電力が発生した状態でロジック100が動作可能となり、その状態でタグリーダから送信されてきたRFID送信指令をループアンテナ107aが受信すれば、SA1によりYESの判断がなされてSA2へ進み、前回のRFID発信から5秒経過したか否かの判断がなされる。5秒経過していない場合にはSA10により、前回発信したRFIDと同じものを発信する処理がなされる。5秒経過している場合には、SA3へ進み、ランダムカウンタのカウント値RをEEPROM103から読出す（抽出する）処理がなされる。このランダムカウンタは、偽RFIDのコードをランダムに生成するためのカウンタであり、後述するSA7～SA9により数値データが更新される。

【0147】

次に制御がSA4へ進み、抽出したカウント値Rに基づいてテーブルを参照し、偽RFIDを割出す処理がなされる。SA4により参照されるテーブルが、図12に示されている。図12は東京都千代田区（図13参照）で販売されるRFIDタグ1aのテーブルを示しており、(a)は、1回で1つのRFIDを発信する単数発信タイプのRFIDタグ1aが記憶しているテーブルである。図12(b)、(c)は、1度に複数（例えば4個）の偽RFIDを発信する複数発信タイプのRFIDタグに記憶されているテーブルである。この複数発信タイプのRFIDタグは、複数種類製造されて販売される。そのうちの2種類のRFIDタグ1aに記憶されているテーブルを図12(b)(c)に示す。複数発信タイプのRFIDタグは、図12(b)(c)からも分かるように、ランダムカウンタの抽出値（乱数）が0～39の範囲のときに検索される4つの偽RFID1～4のうち3つの偽RFID2～4が互いに共通のコードとなっており、1つのRFID1のみ互いに異なるように構成されている。また、ランダムカウンタの抽出値（乱数）が0～39以外の範囲のときに検索される4つの偽RFID1～4は、互いに異なるバラバラなコードとなっている。一方、単数発信タイプのRFIDタグも複数種類製造販売され、ランダムカウンタの抽出値（乱数）が0～39の範囲のときに検索される偽RFIDが互いに共通のコードとなっており、ランダムカウンタの抽出値（乱数）が0～39以外の範囲のときに検索される偽RFIDが互いに異なるバラバラなコードとなっている。

【0148】

前述したランダムカウンタは、SA7により「1」加算更新された後SA8によりその値が100以上になったか否かの判断がなされ、なった場合にはSA9によりランダムカウンタの値を「0」にする処理がなされる。その結果、ランダムカウンタは、0からカウントアップしてその上限である99までカウントアップされたのち、再度0からカウントアップし直すように構成されており、このようなランダムカウンタが数値データを抽出すれば、0～99の範囲内の任意の値（乱数）が抽出されることとなる。図12(a)のテーブルを記憶している単数発信タイプのRFIDタグ1aの場合には、抽出したカウント値（乱数）Rに基づいてそのテーブルを参照し、例えば抽出したランダムカウンタの値Rが0～39の範囲内の値であった場合には、820493176の偽RFIDがSA4により割出されることとなる。また、例えば抽出したランダムカウンタRの値が55～69の範囲内の数値であった場合には、813926081の偽RFIDがSA4により割出されることとなる。同様に、図12(b)に示されたテーブルを記憶している複数発信タイプのRFIDタグ1aの場合には、例えば抽出したランダムカウンタRの値が55～69の範囲内の数値であった場合には、814358231、849137655、788

0 1 5 2 3 3、7 7 9 2 8 8 4 0 1の偽RFIDがSA4により割出されることとなる。また、図12(c)に示されたテーブルを記憶している複数発信タイプのRFIDタグ1-aの場合には、例えば抽出したランダムカウンタRの値が85～99の範囲内の数値であった場合には、7 0 0 9 1 3 5 6 1、7 5 0 0 2 1 2 1 4、7 0 2 0 4 9 3 1 9、8 5 6 1 0 4 9 2 3の偽RFIDがSA4により割出されることとなる。

【0149】

次に制御がSA5へ進み、その割出された偽RFIDをループアンテナ107aから発信する処理がなされる。

【0150】

単数発信タイプのRFIDタグ1-aのそれぞれは、40%の確率で8 2 0 4 9 3 1 7 6 10の共通偽RFIDを発信し(図12(a)参照)、かつそれぞれ15%の確率で、7 3 0 8 5 4 7 0 9の偽RFID、8 1 3 9 2 6 0 8 1の偽RFID、7 9 1 4 0 5 7 3 1の偽RFID、8 3 5 4 0 6 9 1 2等の互いにバラバラな偽RFIDを発信することとなる。その結果、このようなRFIDタグ1-aを複数の個人ユーザが身に付けておれば、毎回ランダムなコードからなる偽RFIDが発信されるものの、40%という1番発信確率の高い8 2 0 4 9 3 1 7 6の偽RFID(以下「共通偽RFID」という)が頻繁に発信されることとなる。その結果、異なった複数場所に設置されたタグリーダーによって読取られたRFIDがたまたま同一コードのRFIDであった場合には、本来なら同一人物から発信されたRFIDと判断できるが、このRFIDタグ1-aが複数の個人ユーザに所持されることにより、複数箇所で同一のRFIDを受信したとしてもそれが異なる人物によって発信された前記共通偽RFIDである可能性も生じる(異人物同一識別子発信現象)。その結果、同一のRFIDを複数箇所で受信したとしても必ずしも同一人物であるとは限らないこととなり、悪意のRFID受信者側の同一人物である旨の推測を攪乱することができ、個人ユーザのプライバシーを保護することができる。

【0151】

図12(a)に示すテーブルを記憶した単数発信タイプのRFIDタグ1-aのみの場合には、そのRFIDタグ1-aを所持する個人ユーザが他にRFIDタグを一切所持していないかあるいは所持してもRFID発信停止状態にしている場合には、前述した攪乱効果が有効に発揮される。しかし、個人ユーザが身に付けている複数の商品それぞれに付されているRFIDタグからRFIDが発信される状態となっている場合には、単数発信タイプのRFIDタグ1-aを所持している状態では、タグリーダーからのRFID送信指令が発せられれば、RFIDタグ1-aからランダムな偽RFIDが発せられるとともに、当該個人ユーザが所持している商品に付されているRFIDタグから毎回同じRFIDが発信されることとなる。その結果、同一人物が或る場所に設置されたタグリーダーに対して複数のRFIDを発信した後他の場所へ移動してそこに設置されているタグリーダーに対し複数のRFIDを発信した場合には、複数のRFIDの内の一つが異なり他のものがすべて同一という現象(複数識別子中1個可変型現象)が生ずる。ただし、偶然すべてのRFIDが一致する状態となることもまれにある。その結果、一度に複数のRFIDを受信した場合には、その内の1つのRFIDが異なり他の全てが一致するかまたは全てのRFIDが一致する場合には、同一人物であると推測されてしまう不都合が生ずる。

【0152】

そこで、図12(a)に示したテーブルを記憶している単数発信タイプのRFIDタグ1-aばかりでなく、図12(b)、(c)に示すようなテーブルを記憶した複数発信タイプのRFIDタグ1-aも合わせて製造販売して個人ユーザに普及させる。

【0153】

具体的には、購入済みの所持品に付されているRFIDタグを発信停止状態等にして自己の所持品からRFIDが他人に読取れないようにしている個人ユーザには、前述の複数発信タイプのRFIDタグ1-aを普及させる。一方、他人が購入済み商品からのRFIDを読取ることができるようになっている個人ユーザに対しては、前述の単数発信タイプのRFIDタグ1-aを提供する。前者の個人ユーザの場合には、前述したように、1つの偽

R F I D がランダムに発信されるとともに所持品に付されている R F I D タグから本物の R F I D が同時に発信されるという現象（複数識別子中 1 個可変型現象）が生ずる。一方、後者の個人ユーザの場合には、1 度に複数（図 1 2 の場合には 4 個）の偽 R F I D 1 ~ 4 がランダムに発信される状態となる。ところが、前述したように、個人ユーザ同士の間で、4 0 % の確率で共通偽 R F I D 2 ~ 4 と 1 つの異なった R F I D 1 とが発信される状態となる。このような現象は、前述の複数識別子中 1 個可変型現象と同じ現象であるが、異なった人物の間でこの複数識別子中 1 個可変型現象が生ずることとなる。その結果、悪意の受信者側に見れば、複数識別子中 1 個可変型現象が生ずれば同一人物であるという推測の信頼性が低下するととなり、同一人物の推測に基づいたプライバシーの侵害が前提から崩れることとなる。

10

【 0 1 5 4 】

次に図 1 1 に戻り、S A 6 により電圧低下が生じたか否かの判断がなされる。これは、電力用の電波の発信が停止して大容量のコンデンサ 1 1 0 に貯えられている電力を使用して R F I D タグ 1 a が作動している状態で、そのコンデンサ 1 1 0 の貯留電力が少なくなつてロジック 1 0 0 に供給される電圧が低下したか否かを判別するものである。電圧が低下したと判別された場合には、S A 1 0 a に進み、現時点のランダムカウンタのカウント値 R が E E P R O M 1 0 3 に記憶された後この偽 R F I D タグの動作がストップする。この S A 1 0 a により記憶されたランダムカウンタのカウント値 R が S A 3 により読出される（抽出される）。一方、電源用の電力が供給されている最中あるいは電源用電力がストップした後コンデンサ 1 1 0 から充分電力が供給されている最中には、S A 6 により N O

20

【 0 1 5 5 】

図 1 3 は、前述した複数種類の偽 R F I D タグ 1 a をグループ分けしてそのグループ毎に地域を指定して販売する地域指定方式の一例を示す説明図である。図 1 3 (a) は、図 1 2 (a) のテーブルを記憶している単数発信タイプの R F I D 1 a の地域指定の一例を示し、図 1 3 (b) は、図 1 2 (b) (c) に示された複数発信タイプの R F I D タグ 1 a の地域指定の一例を示す図である。

【 0 1 5 6 】

図 1 2 (a) に示された 8 2 0 4 9 3 1 7 6 を共通偽 R F I D として発信可能なグループに属する単数発信タイプの R F I D タグ 1 a は、図 1 3 (a) に示すように、東京都千代田区で販売される。また、他のグループに属する 8 0 9 2 0 7 3 2 1 を共通偽 R F I D として発信するグループに属する単数発信タイプの R F I D 1 a は、東京都新宿区で販売される。更に、例えば 7 9 8 0 9 1 3 2 0 を共通偽 R F I D として発信するグループに属する単数発信タイプの R F I D タグ 1 a は、京都市右京区で販売される。

30

【 0 1 5 7 】

一方、複数発信タイプの R F I D タグ 1 a の場合には、図 1 2 (b) (c) に示されたように、7 7 9 2 0 3 9 8 0 , 8 3 9 0 9 3 1 2 7 , 7 4 0 9 8 0 3 4 6 の 3 種類の共通偽 R F I D を 1 度に発信するグループに属する複数発信タイプの R F I D タグ 1 a は、東京都千代田区で販売される。また、他のグループに属する 7 8 8 7 1 8 9 5 5 , 8 4 5 5 9 0 3 2 9 , 8 2 2 7 7 0 9 4 5 を共通偽 R F I D として発信するグループに属する複数発信タイプの R F I D タグ 1 a は、京都市右京区で販売される。

40

【 0 1 5 8 】

尚、地域指定の販売方法としては、その地域内でその地域に対応するグループに属する R F I D タグ 1 a を販売するのに限らず、販売時に使用地域（例えば千代田区、新宿区、右京区等）を表示して、個人ユーザが使用しようと思っている地域の表示を見て選択して購入する方法でもよい。

【 0 1 5 9 】

このように、地域を指定して個人ユーザに提供することにより、共通偽 R F I D が一致する同一グループに属する R F I D タグ 1 a が極力同一地域内で使用されることとなり、

50

同一地域内において同一の共通偽RFIDが発信され易いという傾向が生じ、悪意のプライバシー侵害者を効果的に攪乱できる状態となる。

【0160】

図14は、ブラウザフォン30の動作を説明するためのフローチャートである。S95aにより、RFIDタグ切替処理がなされる。この処理は、個人ユーザが身に付けている購入済み商品に付されているRFIDタグを発信停止状態（識別子ガード状態）または発信再開状態に切替える処理である。S95bにより、偽モード処理がなされる。この処理は、前述のセキュリティ用のRFIDタグ1aの偽RFID発信機能をブラウザフォン30に持たせる処理である。S95cにより、トラップモード処理がなされる。この処理は、個人ユーザが前述のトラップ型VPとして自動決済等を行なう場合にそのトラップ型VP 10
VPに対応する偽RFIDを発信するための処理である。S95dにより、RFID発信処理がなされる。この処理は、タグリーダからRFID発信要求があった場合にブラウザフォン30からRFIDを発信するための処理である。S95により、IC端末使用モードであるか否かの判断がなされる。ブラウザフォン30は、RP用IC端末19RまたはVP用IC端末19Vのうちのいずれか少なくとも一方をUSBポート18に接続していなければ動作しないIC端末使用モードと、IC端末を接続していなくても動作可能なIC
20
端末未使用モードとに切替えることが可能に構成されている。そして、IC未使用モードでない場合にはS96へ進み、その他の処理がなされるが、IC端末使用モードになっている場合には、S97へ進み、VP用IC端末19Vが接続されているか否かの判断がなされ、接続されていない場合にはS98へ進み、RP用IC端末19Rが接続されている
20
か否かの判断がなされ、接続されていない場合すなわち両IC端末ともに接続されていない場合には、制御はS99へ進み、IC端末未使用の警告表示がなされた後S95へ戻る。

【0161】

一方、VP用IC端末19Vが接続されている場合には、制御はS100へ進み、自動決済処理がなされる。この処理については、図31に基づいて後述する。次にS100aにより、ポイントカード登録処理がなされる。これは、百貨店等の業社においてポイントカードを新規発行してもらうための処理である。次に制御はS101へ進み、VP出生依頼処理がなされる。次にS102へ進み、VP用入力処理がなされる。次にS103へ進みVP用決済処理がなされる。

30

【0162】

次に制御がS580へ進み、個人情報の登録処理がなされる。この個人情報の登録処理は、図18(b)に示したVP管理サーバ9の登録処理に対応するブラウザフォン30側の処理である。まずVPとしての本人認証処理を行ない、VP管理サーバ9が本人認証の確認を行なったことを条件として、VPの個人情報を金融機関7のVP管理サーバ9へ送信してデータベース12aに登録してもらう処理を行なう。

【0163】

次に制御がS582へ進み、個人情報の確認処理がなされる。この処理は、金融機関7のVP管理サーバ9とブラウザフォン30との間でなされる処理である。まずVPとしての本人認証がなされ、次に、データベース12aに格納されている自分の個人情報の確認 40
を行なう処理がなされる。一方、確認の結果誤りがある場合あるいは引越しや転職等によって個人情報に変更があった場合には、このS582により、その変更情報が、金融機関7のVP管理サーバ9へ送信される。

【0164】

次に制御がS583へ進み、商品検索・購入処理がなされる。この処理は、図45に基づいて後述する。次に制御がS585へ進み、住所、氏名、Eメールアドレスの送信処理が行なわれる。一方、ブラウザフォン30のUSBポート18にRP用IC端末19Rが接続されている場合には、S98によりYESの判断がなされてS105へ進み、電子証明書発行要求処理がなされる。次に制御がS106へ進み、RP用入力処理がなされる。次にS107へ進み、RP用決済処理がなされる。この処理については、VP用決済処理 50

と類似した制御処理である。

【 0 1 6 5 】

図 1 5 は、S 9 5 a に示した R F I D タグ 切 換 え 処 理 の サ ブ ル ー チ ン プ ロ グ ラ ム を 示 す フ ロ ー チャートである。S B 1 により、O F F 切 換 え 操 作 が あ っ た か 否 か の 判 断 が な さ れ る。切 換 え 操 作 が な い 場 合 に は S B 2 へ 進 み、O N 切 換 え 操 作 が あ っ た か 否 か の 判 断 が な さ れ る。操 作 が な い 場 合 に は こ の サ ブ ル ー チ ン プ ロ グ ラ ム が 終 了 す る。

【 0 1 6 6 】

一 方、個 人 ユ ー ザ が 所 持 し て い る 購 入 済 み 物 品 に 付 さ れ て い る R F I D タ グ を 発 信 停 止 状 態 に す る た め の O F F 切 換 え 操 作 が ブラウザフォン 3 0 に よ り な さ れ た 場 合 に は、S B 1 により Y E S の 判 断 が な さ れ て S B 3 へ 進 み、そ の ブラウザフォン 3 0 か ら パ ス ワード が 購 入 済 み 物 品 に 付 さ れ て い る R F I D タ グ に 発 信 さ れ る。R F I D タ グ は そ の 発 信 さ れ て き た パ ス ワード を 記 憶 す る。次 に S B 4 に 従 っ て ブラウザフォン 3 0 か ら O F F モード 指 令 が 発 信 さ れ る。こ れ を 受 け た R F I D タ グ は、記 憶 し て い る R F I D を 発 信 し な い 状 態 に 切 換 わ る。こ れ に よ り、R F I D タ グ が、個 人 ユ ー ザ の 意 思 に 従 っ て 他 人 が 読 取 れ な い 識 別 子 ガード 状 態 に な る。こ の 識 別 子 ガード 状 態 の 他 の 例 と し て は、R F I D タ グ を アルミ箔等 で 覆 い R F I D を 他 人 が 読 取 れ な い よ う に す る も の で あ っ て も よ い。ま た、R F I D タ グ か ら の R F I D の 読 取 り を 妨 害 す る 妨 害 電 波 等 を 発 信 す る 装 置 を 個 人 ユ ー ザ が 携 帯 し、タ グ リーダ か ら の R F I D 読 取 り 要 求 が あ っ た と き に 妨 害 電 波 等 を 発 信 し て R F I D を 読 取 れ な い よ う に し て も よ い。次 に S B 5 に 従 っ て ブラウザフォン 3 0 か ら R F I D タ グ へ 送 信 指 令 が 発 信 さ れ る。次 に S B 6 へ 進 み、R F I D の 受 信 が あ っ た か 否 か の 判 断 が な さ れ る。S B 4 に 従 っ て O F F モード 指 令 が 既 に 発 信 さ れ て い る た め に、通 常 で は、個 人 ユ ー ザ に 所 持 さ れ て い る 購 入 済 物 品 に 付 さ れ て い る R F I D タ グ か ら R F I D が 発 信 さ れ る こ と は な い。従 っ て、S B 6 に よ り N O の 判 断 が な さ れ て S B 7 に よ り O F F モード 切 換 え 完 了 の 表 示 が ブラウザフォン 3 0 に よ り な さ れ る。と ころ が、S B 4 に よ り O F F モード 指 令 を 発 信 し た に も か か わ ら ず、電 波 状 況 が 悪 か っ た り 何 ら か の 受 信 ミ ス が 発 信 し て 個 人 ユ ー ザ に 所 持 さ れ て い る 購 入 済 み 物 品 に 付 さ れ て い る R F I D が 発 信 停 止 状 態 に 切 換 わ ら な か っ た 場 合 に は、S B 6 に よ り Y E S の 判 断 が な さ れ て S B 8 に 進 み、ブラウザフォン 3 0 に よ り エ ラー 表 示 が な さ れ る。

【 0 1 6 7 】

個 人 ユ ー ザ に 所 持 さ れ て い る 購 入 済 物 品 に 付 さ れ て い る R F I D タ グ が R F I D 発 信 停 止 状 態 に な っ た 後、そ れ を 再 度 発 信 再 開 状 態 に 切 換 え る た め の O N 切 換 え 操 作 が ブラウザフォン 3 0 に よ り 行 な わ れ た 場 合 に は、S B 2 に よ り Y E S の 判 断 が な さ れ て S B 9 へ 進 み、本 人 認 証 用 の パ ス ワード が 発 信 さ れ る。こ の パ ス ワード を 受 信 し た 個 人 ユ ー ザ の 購 入 済 物 品 に 付 さ れ て い る R F I D タ グ は、記 憶 し て い る パ ス ワード と 照 合 し て 一 致 す る か 否 か の 判 断 を 行 な っ て 本 人 認 証 を 行 な う。次 に ブラウザフォン 3 0 は、S B 1 2 に 従 っ て、N O モード 指 令 を 発 信 す る。こ れ を 受 け た 購 入 済 物 品 に 付 さ れ て い る R F I D タ グ は、前 述 し た パ ス ワード の 照 合 に よ っ て 本 人 認 証 が 確 認 で き た こ と を 条 件 と し て O N モード 指 令 を 受 信 す る こ と に よ り、R F I D が 発 信 可 能 な 状 態 に 切 換 わ る。

【 0 1 6 8 】

次 に ブラウザフォン 3 0 か ら、S B 1 1 に し た が っ て R F I D 送 信 指 令 が 発 信 さ れ る。次 に S B 1 2 に よ り、R F I D の 受 信 が あ っ た か 否 か の 判 断 が な さ れ る。適 正 に 本 人 認 証 の 確 認 が で き か つ O N モード 指 令 を 受 信 し て お れ ば 購 入 済 物 品 に 付 さ れ て い る R F I D か ら R F I D が 発 信 さ れ る。そ の 場 合 に は、S B 1 2 に よ り Y E S の 判 断 が な さ れ て S B 1 3 お 進 み、O N モード 切 換 え 完 了 表 示 が ブラウザフォン 3 0 に よ り な さ れ る。一 方、本 人 認 証 が 確 認 で き な か っ た 場 合 や R F I D 送 信 指 令 の 電 波 を 受 信 し 損 な っ た 場 合 に は 購 入 済 み 物 品 に 付 さ れ て い る R F I D タ グ か ら R F I D が 発 信 さ れ な い。そ の 場 合 に は、S B 1 2 よ り N O の 判 断 が な さ れ て S B 8 へ 進 み、ブラウザフォン 3 0 に よ り エ ラー 表 示 が な さ れ る。

【 0 1 6 9 】

図 1 6 は、個 人 ユ ー ザ に 所 持 さ れ て い る 購 入 済 み 物 品 に 付 さ れ て い る R F I D タ グ の 動

作を示すフローチャートである。S C 1により、パスワードを受信したか否かの判断がなされ、受信していない場合にはS C 2へ進み、R F I D送信指令を受信したか否かに判断がなされ、受信していない場合にはS C 1へ戻る。このS C 1→S C 2→S C 1のループの巡回途中でS B 3またはS B 9にしたがってブラウザフォン30からパスワードが発信されてくれば、S C 1によりY E Sの判断がなされてS C 3へ進む。S C 3では、OFFモード指令を受信したか否かの判断がなされ、受信していない場合にはS C 4へ進み、ONモード指令を受信したか否かの判断がなされ、受信していない場合にはS C 3へ戻る。このS C 3→S C 4→S C 3のループの巡回途中で、S B 4にしたがってブラウザフォン30からOFFモード指令が発信されて来れば、S C 3によりY E Sの判断がなされてS C 5へ進み、受信したパスワードを記憶する処理がなされ、S C 6より、OFFモードに切り替える処理がなされてS C 1へもどる。これにより、購入済み物品に付されているR F I Dタグは、記憶しているR F I Dを発信しない発信停止状態に切り替わる。

10

【0170】

一方、S B 10に従ってブラウザフォン30からONモード指令が発信されてくれば、S C 4によりY E Sの判断がなされてS C 7へ進み、受信したパスワードと既に記憶しているパスワードとが一致しているか否かの判断を行なって本人認証を行なう処理がなされる。一致しない場合には、本人認証の確認ができないこととなり、S C 1にもどるが、一致する場合には本人認証の確認ができたと判断してS C 8へ進み、ONモードに切り替える処理がなされる。これにより、購入済み物品に付されているR F I Dタグは、記憶しているR F I Dを発信可能な状態に切り替わる。

20

【0171】

S B 5またはS B 11によりブラウザフォン30からR F I D発信指令があった場合あるいはタグリーダからR F I D送信指令があった場合には、S C 2によりY E Sの判断がなされてS C 9へ進み、ONモード即ち記憶しているR F I Dを発信可能なモードになっているか否かの判断がなされる。ONモードになっていない場合にはS C 1へ戻るが、ONモードになっている場合にはS C 10へ進み、記憶しているR F I Dを発信する処理がなされる。

【0172】

図17は、図2に示したV P管理サーバ9の処理動作を示すフローチャートである。ステップS1により、V Pの出生依頼があったか否かの判断がなされる。顧客（ユーザ）がブラウザフォン30を操作してV Pの出生依頼を行なえば、S1aに進み、正当機関である旨の証明処理がなされる。この証明処理は、金融機関7がV Pの管理をする正当な機関であることを証明するための処理であり、他人が金融機関7になりすます不正行為を防止するための処理である。この処理については、図24（b）に基づいて後述する。次にS2へ進み、R Pの氏名、住所の入力要求をブラウザフォン30へ送信する。次にS3へ進み、R Pの氏名、住所の返信がブラウザフォン30からあったか否かの判断がなされ、あるまで待機する。

30

【0173】

ユーザであるR Pがブラウザフォン30から自分の氏名、住所を入力して送信すれば、S3によりY E Sの判断がなされてS4へ進み、乱数Rを生成してチャレンジデータとしてブラウザフォン30へ送信する処理がなされる。ユーザがV Pの出生依頼を行なう場合には、ブラウザフォン30のUSBポート18にV P用I C端末19Vを差込んでおく。その状態で、V P管理サーバ9から乱数Rが送信されてくれば、その乱数をV P用I C端末19Vへ入力する。すると、後述するように、V P用I C端末19V内において入力された乱数RをR Pの認証鍵K Nを用いて暗号化する処理がなされ、その暗号結果がブラウザフォン30へ出力される。ブラウザフォン30では、その出力されてきた暗号化データであるレスポンスデータIをV P管理サーバ9へ送信する。すると、S5によりY E Sの判断がなされてS6へ進み、R Pの認証鍵K Nを用いて、受信したレスポンスデータIを復号化する処理すなわち $D_k(I)$ を算出する処理がなされる。次にS7へ進み、S4により生成した乱数 $R = D_k(I)$ であるか否かの判断がなされる。

40

50

【 0 1 7 4 】

V P の出生依頼者が金融機関 7 のデータベース 1 2 に記憶されている正規の R P である場合には、 $R = D_{k,s}(I)$ となるために、制御が S 9 へ進むが、データベース 1 2 に記憶されている R P に他人がなりすまして V P の出生依頼を行なった場合には、 $R = D_{k,s}(I)$ とはならないために、制御が S 8 へ進み、アクセス拒絶の旨がブラウザフォン 3 0 へ送信されて S 1 へ戻る。

【 0 1 7 5 】

一方、S 7 により Y E S の判断がなされた場合には、S 9 へ進み、希望のコンビニエンスストアの入力があったか否かの判断がなされる。V P の出生依頼を行なった R P は、誕生してくる V P の住所となるコンビニエンスストアについて特に希望するコンビニエンスストアがあれば、ブラウザフォン 3 0 に入力して V P 管理サーバ 9 へ送信する。その場合には、S 9 により Y E S の判断がなされて S 1 0 へ進み、その入力されてきたコンビニエンスストアの情報を記憶した後 S 1 2 へ進む。一方、希望するコンビニエンスストアの入力がなかった場合には S 1 1 へ進み、R P の住所に近いコンビニエンスストアを検索してそのコンビニエンスストアを記憶した後 S 1 2 へ進む。

【 0 1 7 6 】

S 1 2 では、V P の氏名、V P の住所であるコンビニエンスストアの住所、V P の E メールアドレス等を決定する。次に S 1 3 へ進み、V P の公開鍵の送信要求をブラウザフォン 3 0 へ送信する。そして、S 1 4 へ進み、公開鍵 K P の返信があったか否かの判断がなされ、あるまで待機する。V P の公開鍵の送信要求を受けたブラウザフォン 3 0 は、接続されている V P 用 I C 端末 1 9 V へ公開鍵出力要求を出力する。すると、後述するように、V P 用 I C 端末 1 9 V は、記憶している V P 用の公開鍵 K P をブラウザフォン 3 0 へ出力する。ブラウザフォン 3 0 では、その出力されてきた V P 用の公開鍵 K P を V P 管理サーバ 9 へ返信する。すると、S 1 4 より Y E S の判断がなされて S 1 5 へ進み、R P に対応付けて、V P の氏名、住所、公開鍵 K P、E メールアドレスをデータベース 1 2 へ記憶させる処理がなされる。

【 0 1 7 7 】

次に S 1 6 へ進み、V P の電子証明書を作成して X M L ストア 5.0 に登録する処理がなされる。この電子証明書は、金融機関 7 等の第三者機関において R P との対応関係が登録されている正規の V P であることを証明するものである。次に S 1 7 へ進み、R P に、V P の氏名、コンビニエンスストアの住所、コンビニエンスストアの名称、E メールアドレス、電子証明書を記憶した I C 端末 1 9 I を郵送するための処理がなされる。次に S 1 8 へ進み、S 1 2 で決定された住所のコンビニエンスストアに V P の氏名、E メールアドレス、当該金融機関 7 の名称を送信する処理がなされる。次に S 1 9 へ進み、正当機関である旨の証明処理がなされる。この正当機関である旨の証明処理は、前述した S 1 a と同じ処理である。次に S 1 へ戻る。

【 0 1 7 8 】

本発明でいう「匿名用の電子証明書」とは、ユーザと当該ユーザが用いる匿名（V P 氏名）との対応関係を特定可能な情報を登録している守秘義務のある所定機関（金融機関 7）により発行され、前記匿名を用いるユーザが当該所定機関に登録されているユーザであることを証明する証明書を含む概念である。よって、本人確認に用いる一般的なデジタル I D ばかりでなく、前記所定機関が前記匿名を用いるユーザに対し当該ユーザは当該所定機関に登録されているユーザであることを証明する電子的な証明書をすべて含む概念である。たとえば、ユーザが用いる匿名とその匿名が前記所定機関に登録されているメッセージとに対し、前記所定機関によるデジタル署名が施されただけの、簡単な証明書を含む概念である。

【 0 1 7 9 】

S 1 により N O の判断がなされた場合には図 1 8 (a) の S 4 0 0 へ進む。S 4 0 0 では、個人情報の登録処理が行なわれ、次に S 4 0 1 によりトラップ情報の登録処理が行なわれ、S 4 0 2 により個人情報の確認処理が行なわれ、S 4 0 3 により個人情報の照合、

流通チェック処理が行なわれ、S 4 0 4 により個人情報の販売代行処理が行なわれ、S 4 0 5 によりメール転送、流通チェック処理が行なわれて S 1 へ戻る。ユーザから個人情報の提供を受けたサイト（業者）側では、提供してもらった個人情報が本当に正しい内容であるか否かを確認したいというニーズがある。そこで、金融機関 7 の V P 管理サーバ 9 は、ユーザから個人情報を受付けてその個人情報が正しい個人情報かどうかをチェックし、正しい個人情報のみをデータベース 1 2 a に登録する。その処理を S 4 0 0 により行なう。

【 0 1 8 0 】

一方、ネットワーク上で V P の利用が盛んになった場合には、R P と V P との両方の詳しい個人情報を収集した業者が、両個人情報をしらみつぶしにマッチングして、両個人情報 10
が一致する R P 氏名と V P 氏名とを割出し、V P に対応する R P を予測してしまうという不都合が生ずる恐れがある。そこで、個人情報をデータベース 1 2 a に登録する場合には、勤務先名や所属部署名あるいは役職等の R P が特定されてしまうような個人情報を排除（または変更）して、登録する必要がある。そのような処理を、S 4 0 0 により行なう。

【 0 1 8 1 】

一方、個人情報主であるユーザは、自己の個人情報が正しい内容で流通しているか否かを監視し、間違っていれば正しい内容に修正したいというニーズがある。そこで、データベース 1 2 b に登録されている自己の個人情報の真偽をユーザがチェックできるように、S 4 0 2 により、個人情報の確認処理が行なわれる。

20

【 0 1 8 2 】

さらに、ユーザが自己の個人情報の公開範囲（流通範囲）を限定した上でその個人情報を業者側（サイト側）に提供した場合に、その公開範囲（流通範囲）が守られているか否かを監視したいというニーズがある。個人情報の提供を受けた業者側は、前述したようにその個人情報が正しい情報であるか否かを確認したいというニーズがある。そこで、サイト側（業者側）が所有している個人情報を正しい個人情報が登録されているデータベース 1 2 a の個人情報と照合できるようにする一方、その照合対象となった業者側所有の個人情報の流通許容範囲をチェックして正しく流通されているか否かを確認できるように、S 4 0 3 の処理が行なわれる。

【 0 1 8 3 】

ユーザは、個人情報を提供する見返りとして、何らかのサービスあるいは金銭を入手したいというニーズがある。そこで、S 4 0 4 により、個人情報の販売代行が行なわれる。図 3 に基づいて説明したように、トラップ型 V P は、E メールアドレスを金融機関 7 のトラップ型 V P 用として開設しているアドレスにしているため、そのトラップ型 V P に宛てた E メールは金融機関 7 のトラップ型 V P 用に開設された E メールアドレス宛に送られる。そこで、その送られてきた E メールを対応する V P の E メールアドレスに転送する必要がある。その処理を、S 4 0 5 により行なう。その際に、業者側から送られてくる E メール宛名はトラップ型 V P となっているために、そのトラップ型 V P に対応するサイト（
業社）を割出し（図 3 参照）、その割出されたサイト（業社）からの E メールでなかった
場合には当該トラップ型 V P の個人情報の流通許容範囲内のサイト（業社）からの E メール 40
か否かを確認し、流通チェックを行なうことも、S 4 0 5 により行なわれる。

【 0 1 8 4 】

図 1 8 （b）は、S 4 0 0 の個人情報の登録処理のサブルーチンプログラムを示すフローチャートである。この個人情報の登録処理は、ユーザが V P として個人情報を登録する際の処理である。

【 0 1 8 5 】

乱数 R を受信したブラウザフォン 3 0 は、そのブラウザフォン 3 0 に接続されている V P 用 I C 端末 1 9 V に記憶されている V P 用の秘密鍵を用いて乱数 R を 1 回暗号化してレスポンスデータ I を生成する。そしてそのレスポンスデータ I を金融機関 7 の V P 用管理サーバ 9 へ送信する。

50

【 0 1 8 6 】

S 4 1 0 により、ユーザ側から個人情報の登録要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。登録要求があった場合には S 4 1 1 へ進み、正当機関証明処理がなされる。次に制御が S 4 1 2 へ進み、V P の氏名の入力要求がなされ、S 4 1 3 により入力があったか否かの判断がなされる。入力があった場合には制御が S 4 1 4 へ進み、乱数 R を生成してチャレンジデータとして登録要求を行なったユーザ側に送信する処理がなされる。S 4 1 5 へ進み、ユーザ側からレスポンスデータ I を受信したか否かの判断がなされ、受信するまで待機する。受信した段階で S 4 1 6 へ進み、V P の公開鍵 K P をデータベース 1 2 a から検索して、受信したレスポンスデータ I を公開鍵 K P で暗号化した $D_{K_P}(I)$ を生成する処理がなされる。

10

【 0 1 8 7 】

次に制御が S 4 1 7 へ進み、チャレンジデータ R と $D_{K_P}(I)$ が等しいか否かの判断がなされる。等しくなければユーザの本人認証ができなかったこととなり S 4 2 2 へ進み、登録拒否の処理がなされる。S 4 1 7 により Y E S の判断がなされた場合には制御が S 4 1 8 へ進み、登録要求を出したユーザに対し登録を希望する個人情報の入力要求を出す処理がなされる。次に S 4 1 9 へ進み、入力があったか否かの判断がなされ、入力があるまで待機する。入力があった段階で制御が S 4 2 0 へ進み、登録対象の個人情報の真偽チェックを行なう。

【 0 1 8 8 】

この真偽チェックは、たとえば、X M L ストア 5 0 にアクセスして該当するユーザの個人情報 20 が登録されている場合にそれと照合チェックしたり、電子行政群 4 9 に含まれる市役所等にアクセスしてそこに登録されている個人情報と照合チェックしたりして行なわれる。このような機械検索による照合チェックだけでは不十分な場合には、金融機関 7 の調査員が裏取り調査を行なって真偽チェックを行なう。

【 0 1 8 9 】

次に制御が S 4 2 1 へ進み、真偽チェックの結果正しいか否かの判断がなされ、正しくない場合には S 4 2 2 へ進み登録拒否の処理がなされる一方、正しい場合には S 4 2 3 へ進み、R P が特定される個人情報か否かの判断がなされる。登録しようとしている V P の個人情報の中に、たとえば勤務先名や所属部署名あるいは役職等の R P が特定されてしまうような個人情報が存在する場合に、それをそのまま登録してしまうと、その登録情報 30 からどの V P がどの R P に対応するかを第三者に予測されてしまう恐れがある。このデータベース 1 2 a に登録される個人情報は、S 4 0 3 や S 4 0 4 によりサイト側（業者側）が知り得る状態となる。その結果、サイト側（業者側）に、R P と V P との対応関係が予測される恐れが生ずる。

【 0 1 9 0 】

そこで、S 4 2 3 により、R P が特定される個人情報か否かの判断がなされ、予測される個人情報でなければ S 4 2 5 へ進むが、予測される恐れのある個人情報の場合には S 4 2 4 へ進み、その個人情報を加工する処理がなされた後 S 4 2 5 へ進む。たとえば、勤務先名が M E C であった場合には、それをたとえば「某大手電気メーカー」に加工したり、役職がたとえば専務であった場合には、たとえば「重役」に加工したりする。

40

【 0 1 9 1 】

S 4 2 5 では、個人情報に当該金融機関のデジタル署名を付してユーザ名別に登録する処理がなされる。その結果、図 4 に示すようなデータがデータベース 1 2 a に登録される。

【 0 1 9 2 】

図 1 9 は、S 4 0 1 に示されたトラップ情報の登録処理のサブルーチンプログラムを示すフローチャートである。S 4 3 0 により、正当機関証明処理がなされ、S 4 3 1 により、V P 氏名の入力要求がトラップ情報の登録依頼をしてきた V P に出される。次に S 4 3 2 へ進み、その登録依頼をしてきた V P が自己の V P 氏名を入力したか否かの判断がなされ、入力するまで S 4 3 1 の要求が出される。次に制御が S 4 3 3 へ進み、乱数 R を生成 50

してチャレンジデータとして登録依頼者であるVPに送信する処理がなされる。S 4 3 4により、レスポンスデータIを受信したか否かの判断がなされる。

【 0 1 9 3 】

送信されてきたチャレンジデータRを受信した登録依頼者であるVPがそのチャレンジデータRを自己の秘密鍵で暗号化してレスポンスデータIを生成し、金融機関7のVP管理サーバ9へ送信する。すると、制御がS 4 3 5へ進み、登録依頼をしてきたVPの公開鍵KPをデータベース1 2 aから検索し、受信したレスポンスデータIをその公開鍵KPで復号化する処理を行なう。そしてS 4 3 6により、チャレンジデータR=D_k(I)であるか否かの判断がなされ、イコールでない場合には認証の結果そのVPが本人と確定できないということであり、S 4 3 7により登録拒否の通知がそのVPになされる。一方、S 4 3 6によりYESの判断がなされて認証の結果VPが本人であることが確認できた場合には、制御がS 4 3 8へ進み、トラップ情報の送信要求をそのVPへ送信する処理がなされる。

【 0 1 9 4 】

VPから登録してもらいたいトラップ情報が送信されてきたか否かがS 4 3 9によりなされ、送信されてくるまで待機する。送信されてきた段階で制御がS 4 4 0へ進み、送信されてきたトラップ情報をデータベース1 2 aに記憶させる処理がなされる。このトラップ情報は、登録依頼者であるVPに対応した記憶領域に記憶される。次に制御がS 4 4 1へ進み、そのトラップ情報に対する電子署名を金融機関7が生成して、その電子証明書をXMLストア5 0へ登録する処理がなされる。その結果、図5に基づいて説明したように、XMLストア5 0のデータベース7 2に電子証明書が格納される。

【 0 1 9 5 】

この電子証明書は、XMLストア5 0に格納する代わりに登録依頼を行なってきたVPのIC端末1 9 Vに格納してもよい。しかし、トラップ情報は、前述したように、そのVPがアクセスしたWebサイト毎またはVP（トラップ型VP）として登録してポイントカードを新規発行してもらった百貨店等の業社毎に異なり、その結果電子証明書もWebサイト毎（業社毎）に異なることとなり、多数の電子証明書をIC端末1 9 Vに格納するとなると、記憶容量の問題が生ずる。ゆえに、本実施の形態では、その記憶容量の問題を克服するために、XMLストア5 0へ登録する。なお、IC端末1 9 Vの記憶容量が非常に大きなものであれば、金融機関7が発行した電子証明書のすべてまたはその大半をこのIC端末1 9 Vに記憶させてもよい。

【 0 1 9 6 】

図2 0は、S 4 0 5に示されたメール転送、流通チェックのサブルーチンプログラムを示すフローチャートである。S 5 1 4により、サイト（業者）からメールが送られてきたか否かの判断がなされる。図3等に基づいて説明したように、VPが、本名を用いてサイトにアクセスしたり業社にポイントカードを登録した場合にはVP自身のEメールアドレスをそのサイト側（業社側）に通知するが、トラップ型VP氏名を用いてサイト（業社）にアクセスした場合には、金融機関7のトラップ型VP用として開設されているEメールアドレスをそのサイト（業社）側に提供する。その結果、そのサイト（業社）からのEメールは、金融機関7のトラップ型VP用に開設されたEメールアドレスで送られてくることとなる。

【 0 1 9 7 】

金融機関7では、そのトラップ型VP用に開設したEメールアドレスに送信されてきたメールがある場合には、VP管理用サーバ9は、S 5 1 4により、YESの判断を行なう。その結果、制御がS 5 1 5へ進み、その送られてきたEメールに含まれている宛名に対応するサイト名（業者名）をデータベース1 2 aから割出す処理を行なう。データベース1 2 aは、図3に基づいて説明したように、VPの氏名とそのVPがアクセスしたサイト名（業社名）とが対応付けられて記憶されている。この対応関係を利用して、メールの宛名から対応するサイト名（業者名）を割出す処理がなされる。

【 0 1 9 8 】

次に S 5 1 6 により、割出されたサイト名（業社名）と E メールを送ったサイト名（業社名）とが一致するか否かの判断がなされる。本来なら一致する筈であるが、個人情報不正に流通された場合には、その不正流通された個人情報を不正入手したサイト（業社）がその個人情報主に E メールを送る場合がある。その場合には、割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない状態となる。

【 0 1 9 9 】

割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない場合に、即座に個人情報が不正流通されたとは断定できない。サイト（業社）側に個人情報を提供する際に、ある一定の流通許容範囲内においては流通させてもよいと個人情報主であるユーザから承諾を得ている場合がある。よって、S 5 2 2 に制御が進み、XML ストアの該当個人情報を検索して、ポリシーに定められている流通許容範囲内に E メール送信者が含まれるか否かチェックする処理がなされ、S 5 2 3 により、含まれると判断された場合には制御が S 5 1 7 へ進むが、含まれないと判断された場合には制御が S 5 1 9 へ進む。

【 0 2 0 0 】

S 5 1 9 では、E メールを送ったサイト名（業社名）に対応させて個人情報の不正入手値を「1」加算更新する処理がなされ、S 5 2 0 により、S 5 1 5 によって割出されたサイト名（業社名）に対応させて個人情報の不正流出値を「1」加算更新する処理がなされる。次に S 5 2 1 により、個人情報の不正があった旨およびその詳細データを該当するユーザへ通知する処理がなされる。

【 0 2 0 1 】

一方、個人情報不正流通されていないと判断された場合には制御が S 5 1 7 へ進み、Eメールの宛名に対応するユーザのメールアドレスを割出す処理がなされ、S 5 1 8 により、その割出されたアドレスに E メールを転送する処理がなされる。

【 0 2 0 2 】

図 2 1 は、図 2 に示した認証用サーバ 1 1 の処理動作を示すフローチャートである。先ず S 2 5 により、RP から電子証明書の発行依頼があったか否かの判断がなされ、あるまで待機する。ユーザである RP がブラウザフォン 3 0 から RP の電子証明書の発行依頼要求を認証用サーバ 1 1 へ送信すれば、制御が S 2 6 へ進み、RP の住所、氏名、公開鍵の送信要求をブラウザフォン 3 0 へ送信する処理がなされる。次に S 2 7 へ進み、ブラウザフォン 3 0 から RP の住所、氏名、公開鍵の返信があるか否かの判断がなされ、あるまで待機する。そして、返信があった段階で制御が S 2 8 へ進み、RP の電子証明書を作成してブラウザフォン 3 0 へ送信する処理がなされる。次に S 2 9 へ進み、RP の住所、氏名、公開鍵 KP をデータベース 1 2 a に記憶する処理がなされて S 2 5 へ戻る。

【 0 2 0 3 】

図 2 2 ～ 図 2 4 は、図 2 の決済サーバ 1 0 の処理動作を示すフローチャートである。S 3 5 により、RP の銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合には S 3 9 へ進み、VP の銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合には S 4 0 へ進み、デビットカードの発行依頼があったか否かの判断がなされ、ない場合には S 4 1 へ進み、決済依頼があったか否かの判断がなされ、ない場合には S 3 5 へ戻る。

【 0 2 0 4 】

この S 3 5 ～ S 4 1 のループの巡回途中で、ユーザが金融機関 7 へ出向き、RP の銀行口座の開設依頼を行なって RP の銀行口座番号の作成依頼が入力されれば、制御が S 3 6 へ進み、RP の住所、氏名等の入力要求がなされ、入力があれば制御が S 3 8 へ進み、RP の銀行口座を作成して、データベース 1 2 a に記憶するとともに RP に通知する処理がなされて S 3 5 へ戻る。

【 0 2 0 5 】

ユーザが金融機関 7 へ出向き、VP の銀行口座の開設依頼を行なって VP の銀行口座番号の作成依頼要求が入力されれば、S 4 2 へ進み、VP の住所、氏名等、RP の住所、氏

名等の入力要求がなされる。ユーザは、これら情報を手動でキーボードから入力するか、または、決済サーバ10にRP用IC端末19RやVP用IC端末19Vを接続してこれらデータを自動入力する。データが入力されれば、制御がS44へ進み、RPとVPの対応が適正であるか否かが、データベース12aを検索することにより確認される。

【0206】

RPとVPの対応が適正でない場合にはS51へ進み、対応が不適正である旨を報知してS35へ戻る。一方、RPとVPとの対応が適正な場合にはS45へ進み、VPの銀行口座を作成して、データベース12aに記憶するとともに、VPに対応するRPにその銀行口座を郵送する処理がなされた後S35へ戻る。

【0207】

ユーザが金融機関7へ出向き、デビットカードの発行要求の依頼を行なってデビットカードの発行要求の入力があれば、S40によりYESの判断がなされてS46へ進み、口座番号と氏名と暗証番号の入力要求がなされる。ユーザがRP用のデビットカードの発行を要求する場合には、RPの銀行口座番号と氏名と暗証番号を入力する。一方、ユーザがVP用のデビットカードの発行要求を希望する場合には、VPの銀行口座番号とVPの氏名とVPの暗証番号とを入力する。これらのデータの入力は、RP用IC端末19RまたはVP用IC端末19Vを決済サーバ10へ接続して自動的に入力する。

【0208】

これらデータの入力が行なわれれば制御がS48へ進み、入力データをデータベース12aへ記憶するとともに、デビットカードを発行する処理がなされる。次にS49へ進み、発行されたデビットカードの記憶データをRP用IC端末またはVP用IC端末へ伝送する処理がなされてS35へ戻る。

【0209】

決済サーバ10に決済要求が送信されてくれば、S41によりYESの判断がなされてS50へ進み、決済処理がなされた後S35へ戻る。

【0210】

図23は、図22に示したS50の決済処理のサブルーチンプログラムを示すフローチャートである。決済要求には、銀行口座内の資金を一部RP用IC端末19RまたはVP用IC端末19Vに引落す引落し要求と、デビットカードを使用しての決済要求と、クレジットカードを使用して決済を行なった場合のクレジットカード発行会社からのクレジット使用金額の引落し要求とがある。まずS55よりIC端末19Rまたは19Vへの引落し要求があったか否かの判断がなされ、ない場合にはS57へ進み、デビットカードを使用しての決済要求があったか否かの判断がなされ、ない場合にはS58へ進み、クレジットカード発行会社からの引落し要求があったか否かの判断がなされ、ない場合にはS554へ進み、クレジットカード発行会社からの問合せ処理が行なわれた後、S59によりその他の処理がなされてこのサブルーチンプログラムが終了する。

【0211】

ユーザがブラウザフォン30等からRP用IC端末19RまたはVP用IC端末19Vへ資金の一部引落し要求を決済サーバ10へ送信した場合には、S55によりYESの判断がなされてS56へ進み、正当機関証明処理がなされた後S60へ進む。S60では、氏名を入力要求をブラウザフォン30等へ送信する処理がなされる。その要求を受けたブラウザフォン30では、接続されているIC端末19Rまたは19Vに対し氏名の出力要求を伝送する。すると、接続されているIC端末19Rまたは19Vから氏名がブラウザフォン30へ伝送され、その伝送されてきた氏名をブラウザフォン30が決済サーバ10へ伝送する。すると、S61によりYESの判断がなされてS62へ進み、乱数Rを生成してチャレンジデータとしてブラウザフォン30へ送信する処理がなされる。

【0212】

その乱数Rを受けたブラウザフォン30は、後述するように、接続されているIC端末19Rまたは19Vに対し乱数Rを伝送する。乱数Rを受取ったIC端末がRP用IC端末19Rの場合には、記憶している認証鍵KNを用いてRを暗号化してレスポンスデータ

I を生成し、それをブラウザフォン 30 へ出力する。ブラウザフォン 30 では、その出力されてきたレスポンスデータ I を決済サーバ 10 へ送信する。一方、乱数 R を受取った IC 端末が VP 用 IC 端末 19 V の場合には、受取った乱数 R を記憶している公開鍵 KP を用いて暗号化してレスポンスデータ I を生成し、ブラウザフォン 30 へ出力する。ブラウザフォン 30 では、その出力されてきたレスポンスデータ I を決済サーバ 10 へ送信する。

【 0 2 1 3 】

レスポンスデータ I が送信されてくれば、S 6 3 により YES の判断がなされて S 6 4 に進み、S 6 0 に応じて入力された氏名が RP のものであるか否かが判別され、RP の場合には S 6 5 へ進み、RP の認証鍵 KN をデータベース 12 から検索してその認証鍵 KN を用いて受信したレスポンスデータ I を復号化する処理すなわち $D_{K_N}(I)$ を生成する処理がなされる。次に S 6 6 へ進み、 $R = D_{K_N}(I)$ であるか否かの判断がなされる。IC 端末への引落とし要求を行なったユーザがデータベース 12 に登録されている適正なユーザである場合には、 $R = D_{K_N}(I)$ となるはずであるが、データベース 12 に登録されているユーザになりすまして銀行口座の資金の一部を引落としするという不正行為が行われた場合には、R と $D_{K_N}(I)$ とが一致しない状態となる。その場合には制御が S 7 9 へ進み、不適正である旨をブラウザフォン 30 へ返信する処理がなされてサブルーチンプログラムが終了する。

【 0 2 1 4 】

一方、 $R = D_{K_N}(I)$ の場合には制御が S 6 7 へ進み、引落とし額の入力要求をブラウザフォン 30 へ送信する処理がなされ、引落とし額がブラウザフォン 30 から送信されてくれば、制御が S 6 9 へ進み、RP の口座から引落とし額 G を減算して G をブラウザフォン 30 へ送信する処理がなされてサブルーチンプログラムが終了する。

【 0 2 1 5 】

一方、ユーザが VP として VP 用 IC 端末 19 V への引落としを行なう場合には、VP の本名を用いる。入力された氏名が VP の本名であった場合には S 6 4 により NO の判断がなされて制御が図 2 4 (a) の S 8 5 へ進む。S 8 5 では、VP の公開鍵 KP をデータベース 12 から検索してその公開鍵 KP を用いて受信したレスポンスデータ I を復号化する処理すなわち $D_{K_P}(I)$ を生成する処理がなされる。次に S 8 6 へ進み、 $R = D_{K_P}(I)$ であるか否かの判断がなされる。引落とし要求を行なっているものがデータベース 12 に登録されている VP になりすまして引落とすという不正行為を行なっている場合には、S 8 6 により NO の判断がなされて S 7 9 に進み、不適正である旨がブラウザフォン 30 へ返信されることとなる。一方、S 8 6 により YES の判断がなされた場合には S 8 7 へ進み、引落とし額 G の入力要求をブラウザフォン 30 へ送信する処理がなされ、ブラウザフォン 30 から引落とし額 G の送信があれば、S 8 9 へ進み、VP の銀行口座から G を減算して G をブラウザフォン 30 へ送信する処理がなされた後サブルーチンプログラムが終了する。

【 0 2 1 6 】

ユーザがデビットカードを使用しての決済を行なうべくデビットカード使用操作を行なった場合には、デビットカード使用要求が決済サーバ 10 へ送信され、S 5 7 により YES の判断がなされて S 5 6 へ進み、正当機関証明処理がなされる。次に S 7 0 へ進み、暗証番号とカード情報入力要求がユーザのブラウザフォン 30 へ送信される。デビットカードの暗証番号とデビットカード情報とがブラウザフォン 30 から決済サーバ 10 へ送信されてくれば制御が S 7 2 へ進み、その送信されてきたデータが適正であるか否かの判断がなされ、不適正であれば S 7 9 へ進む。

【 0 2 1 7 】

一方、適正である場合には S 7 3 へ進み、使用額 G の入力待。ユーザが使用額 G を入力してそれが決済サーバ 10 へ送信されてくれば制御が S 7 4 へ進み、該当する口座を検索して G を減算するとともに G をユーザのブラウザフォン 30 に送信する処理がなされる。

【 0 2 1 8 】

ユーザがRPまたはVPの本名を用いて後述するようにクレジットカードによるSETを用いた決済を行なった場合には、クレジットカード発行会社4（図1参照）からクレジット支払金額の引落し要求が決済サーバ10へ送信される。その引落し要求が送信されてくればS58によりYESの判断がなされてS56の正当機関証明処理がなされた後S75へ進み、ユーザの氏名、口座番号の入力を待つ。クレジットカード発行会社4からユーザの氏名と口座番号とが送信されてくれば制御がS76へ進み、その入力されたデータが適正であるか否かをデータベース12を検索して判別する。不適正の場合にはS79へ進むが、適正な場合にはS77へ進み、引落し額Gの入力を待機する。クレジットカード発行会社4から引落し額Gすなわちクレジット支払額と手数料との合計金額が送信されてくれば制御がS78へ進み、口座からGを減算してクレジットカード発行会社の口座Gに加算する処理すなわち資金の移動処理がなされる。

【0219】

S58によりNOの判断がなされた場合にはS554によるクレジット発行会社4からの問合せ処理が行なわれた後S59へ進み、その他の処理が行なわれる。

【0220】

図24（b）は、前述したS1a, S19, S56に示された正当機関証明処理のサブルーチンプログラムを示すフローチャートである。まずS90により、当該機関の電子証明書を送信する処理がなされる。この電子証明書を受信した側においては、乱数Rを生成してその乱数Rを送信する。すると、S91によりYESの判断がなされてS92へ進み、その受信した乱数Rを当該機関の秘密鍵KSで暗号化する処理すなわち $L = E_K(R)$ を算出する処理がなされ、その算出されたLを返信する処理がなされる。

【0221】

このLを受信した受信側においては、既に受信している電子証明書内の当該機関の公開鍵KPを利用してLを復号化することによりRを得ることができる。そのRと送信したRとがイコールであるか否かをチェックすることにより、正当機関であるか否かをチェックすることが可能となる。これについては後述する。

【0222】

図25は、S554に示されたクレジットカード会社からの問合せ処理のサブルーチンプログラムを示すフローチャートである。前述したように、VPがトラップ型VPとしてサイトにアクセスして電子ショッピング等を行なったりトラップ型VPとして登録している小売店等の業社で自動決済を行ってクレジット決済を行なった場合には、VP本人のクレジット番号が用いられるのではなく、そのVP本人のクレジット番号を何回か秘密鍵で暗号化した暗号化クレジット番号が用いられることとなる。たとえば、図3に示すように、トラップ型VP氏名E（B13P）としてサイトMPPにアクセスしたVPは、電子ショッピング等を行なってクレジット決済をする際には、バーチャルクレジット番号E（3288）を用いる。VPは、クレジットカード発行会社4に対し3288のクレジット番号は登録しているが、E（3288）の暗号化クレジット番号までは登録していない。よって、E（3288）のバーチャルクレジット番号がクレジット決済に伴ってクレジットカード発行会社4に送信されてきた場合には、クレジットカード発行会社4は、そのE（3288）のバーチャルクレジット番号を自社で検索して真偽を確かめることはできない。

【0223】

そこで、そのような場合に、クレジットカード発行会社は、金融機関7にそのバーチャルクレジット番号が正しいか否かの照会を行なってもらうのである。

【0224】

クレジットカード発行会社からの問合せがあれば制御はS561へ進み、S561～S568の前述したものと同様の認証処理が行なわれる。認証の結果本人が確認されればS567によりYESの判断がなされてS569へ進み、照会対象データの入力要求がクレジットカード発行会社4に送信される。この照会対象データとは、前述したバーチャルクレジット番号とトラップ型VP氏名とを含む。このトラップ型VP氏名をも入力されること

により、そのトラップ型 V P 氏名とバーチャルクレジット番号とが対応しているか否か等も照会できる。

【 0 2 2 5 】

照会対象データがクレジットカード発行会社から送信されてくれば制御は S 5 7 1 へ進み、データベース 1 2 a を検索してその送信されてきた照会対象データと照合する処理がなされる。次に S 5 7 2 により、照合結果送られてきた照会対象データが適正であるか否かの判断がなされ、適正な場合に S 5 7 3 により、適正な旨をクレジットカード発行会社へ返信し、照合結果適正でない場合には S 5 7 4 により、不適正な旨がクレジットカード発行会社に返信される。S 5 7 3 による適正な旨を返信する際には、S 5 7 0 により入力された照会対象データに対し適正な旨を表わす金融機関 7 側のデジタル署名を付し、そのデジタル署名付きデータが問合せをしたクレジットカード発行会社 4 へ返信されることとなる。 10

【 0 2 2 6 】

図 2 6 は、図 1 4 の S 9 5 b に示されたブラウザフォン 3 0 の偽モード処理のサブルーチンプログラムを示すフローチャートである。S D 1 により、電源投入時であるか否かの判断がなされ、電源投入時でない場合には S D 2 に進み、偽モード操作があったか否かの判断がなされ、ない場合には S D 3 へ進み、偽モード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【 0 2 2 7 】

ブラウザフォン 3 0 の電源が投入されれば S D 1 により Y E S の判断がなされて S D 4 へ進み、現在のモードの種類をブラウザフォン 3 0 により表示する処理がなされる。ブラウザフォン 3 0 のモードは、偽モード、トラップモード、通常モードの 3 種類があり、現在どのモードになっているかが、S D 4 により表示される。次に制御が S D 5 へ進み、現在偽モードになっているか否かの判断がなされ、偽モードになっていない場合にはこの偽モード処理のサブルーチンプログラムが終了する。 20

【 0 2 2 8 】

一方、偽モードになっている場合には S D 6 へ進み、本人認証のためのパスワードを発信させて個人ユーザが所持している購入済物品に付されている R F I D タグに記憶させる処理がなされる。次に R F I D に O F F モード指令を発信する処理が S D 7 により行なわれる。これにより、購入済物品に付されている R F I D タグが、前述したように O F F モード即ち記憶している R F I D を発信しない発信停止モードとなる (S C 6 参照)。次に S D 8 へ進み、購入済物品に付されている R F I D タグに対し R F I D 送信指令を発信し、S D 9 により、その R F I D タグから R F I D が発信されてそれを受信したか否かの判断がなされる。通常であれば、発信停止モードに切換わった後であるために R F I D は発信されてくることがなく、S D 1 0 へ進み、R F I D 交換処理がなされる。一方、S D 9 により R F I D を受信した旨の判断がなされた場合には、S D 1 1 へ進み、ブラウザフォン 3 0 によりエラー表示がなされる。 30

【 0 2 2 9 】

個人ユーザがブラウザフォン 3 0 により偽モード操作を行なった場合には、S D 2 により Y E S の判断がなされて S D 1 2 へ進み、ブラウザフォン 3 0 を偽モードに切換える処理がなされた後に S D 6 へ進む。一方、ブラウザフォン 3 0 により偽モード解除操作が行われた場合には、S D 3 により Y E S の判断がなされて、S D 1 3 へ進み、ブラウザフォン 3 0 の偽モードを解除して通常モードにする処理がなされる。 40

【 0 2 3 0 】

尚、この偽 R F I D 発信機能を有するブラウザフォン 3 0 を有する個人ユーザは、前述のセキュリティ用の R F I D タグ 1 a を必ずしも所持する必要はない。ブラウザフォン 3 0 がセキュリティ用の R F I D タグ 1 a の代わりをしてくれるためである。

【 0 2 3 1 】

図 2 7 は、S D 1 0 に示された R F I D 交換処理のサブルーチンプログラムを示すフローチャートである。S E 1 により、交換希望電波をブラウザフォンから発信する処理がな 50

される。この交換希望電波は、最大20メートルの範囲までしか到達しない電波である。尚、この交換希望電波の到達距離を手動操作により変更設定地点例えば2メートル或いは5メートル等のように変更できるように構成してもよい。次にSE2に進み、交換エリア内即ち交換希望電波が到達する圏内から交換希望電波を受信したか否かの判断がなされる。受信した場合には、SE3へ進み、今日既に交換済みの相手（ブラウザフォン30）であるか否かの判断がなされ、既に交換済みのブラウザフォン30の場合には、交換処理を行なうことなくこのサブルーチンプログラムが終了する。交換済みの相手（ブラウザフォン30）であるか否かの判断を可能にするべく、前述の交換希望電波とともにブラウザフォン30を特定するためのIDコード等を送信してもよい。

【0232】

10

一方、今日まだRFIDの交換を行なっていない相手（ブラウザフォン30）の場合には制御がSE4へ進み、偽RFIDを記憶しているか否かの判断がなされる。ブラウザフォン30のEEPROM194に偽RFIDを記憶しておれば、制御がSE8へ進み、その記憶している偽RFID（たとえば記憶中の1番新しい偽RFID）を交換相手のブラウザフォン30に発信すると共に、相手のブラウザフォン30から偽RFIDを受信する処理がなされる。次にSE9へ進み、EEPROM194に既に記憶している偽RFIDを1つずつ古い記憶エリア側にシフトし、記憶上限を超えた1番古い偽RFIDを消去する処理がなされる。次にSE10へ進み、1番新しい記憶エリアに受信した偽RFIDを記憶する処理がなされる。

【0233】

20

一方、EEPROM194に偽RFIDを全く記憶していない場合には制御がSE5へ進み、個数決定用乱数KRを生成して偽RFIDの送信個数を決定する処理がなされる。次にSE6へ進み、その決定された個数だけのRFIDのコードを決定するための乱数IDRを生成して偽RFIDのコードを決定して発信する処理がなされる。次にSE7へ進み、相手からの偽RFIDを受信して1番新しい記憶エリアに記憶する処理がなされる。

【0234】

このRFID交換処理により、ブラウザフォン30を所持している個人ユーザが例えばすれ違う時に記憶している互いの偽RFIDが交換されて記憶されることとなる。その結果、比較的同じ場所を移動する個人ユーザ同士で偽RFIDを交換しあって互いの共通偽RFIDとして記憶して、RFID送信要求があった場合にはその共通偽RFIDを発信30
することができ、比較的同じ場所を移動する個人ユーザ同士で前述の異人物同一識別子発信現象を生じさせることができ、悪意のプライバシー侵害者を有効に攪乱することができる。

【0235】

図28は、図14のS95cに示されたトラップモードを処理のサブルーチンプログラムを示すフローチャートである。SF1により、トラップモード操作があったか否かの判断がなされ、ない場合にはSF2へ進み、トラップモード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。個人ユーザが自己のブラウザフォン30を操作してトラップモード操作を行なった場合には、SF1によりYESの判断がなされてSF3へ進み、ブラウザフォン30はトラップモードに切換わる。40

【0236】

次にSF4へ進み、当該ユーザが所持している購入済物品に付されているRFIDに対しパスワードを発信する処理がなされる。次にSF5へ進み、OFFモード指令がそのRFIDへ発信される。次にSF6により、RFID送信指令が発信され、SAF7により、RFIDの受信があったか否かの判断がなされる。SF5により既にOFFモード指令が発信されているために、当該ユーザが所持する購入済物品に付されているRFIDタグからRFIDが発信されることは通常あり得ない。よって、通常は、SF7によりNOの判断がなされて、制御がSF7aに進む。SF7aでは、業社選択指定操作があるか否かの判断がなされる。ない場合にはSF8へ進み、個人ユーザが自己のブラウザフォン30により罫を仕掛ける相手業社を選択指定した場合には、制御がSF7bに進み、選択指定50

された業者を記憶する処理がなされた後に S F 8 へ進む。

【 0 2 3 7 】

次に、S F 8 により、トラップモード切換え完了の表示がブラウザフォン 3 0 によりなされる。一方、S F 7 により R F I D の受信があったと判断された場合には S F 9 へ進み、ブラウザフォン 3 0 によりエラー表示がなされる。

【 0 2 3 8 】

次に、個人ユーザが自己のブラウザフォン 3 0 を操作してトラップモード解除操作を行った場合には、S F 2 により Y E S の判断がなされて S F 1 0 へ進み、当該ブラウザフォン 3 0 のトラップモードが解除される。

【 0 2 3 9 】

図 2 9 は、図 1 4 の S 9 5 d に示された R F I D 発信処理のサブルーチンプログラムを示すフローチャートである。S G 1 により、R F I D 送信指令を受信したか否かの判断がなされる。受信していなければこのサブルーチンプログラムが終了する。一方、タグリーダから R F I D 送信指令が発信されれば、ブラウザフォン 3 0 がそれを受信して S G 1 により Y E S の判断がなされ、S G 2 により、受信した旨の報知がブラウザフォン 3 0 によりなされる。この報知は、具体的には、ブラウザフォン 3 0 から受信音を発生させると共に R F I D 送信要求の電波を受信した旨の表示を液晶表示画面に示す。

【 0 2 4 0 】

次に制御が S G 3 へ進み、偽モードになっているか否かの判断がなされる。偽モードになっていない場合には S G 4 へ進み、トラップモードになっているか否かの判断がなされる。トラップモードになっていない場合即ち通常モードの場合にはこのサブルーチンプログラムが終了する。従って、通常モードの場合には、R F I D 送信指令を受信したとしても、何ら R F I D を発信する処理が行なわれない。

【 0 2 4 1 】

ブラウザフォン 3 0 は偽モードになっている場合には S G 3 により Y E S の判断がなされて制御が S G 3 a へ進み、前回の R F I D の発信から 5 秒経過しているか否かの判断がなされる。5 秒経過していない場合には S G 3 b へ進み、前回発信した R F I D と同じコードの R F I D を発信する処理がなされる。これは、タグリーダの読取り信頼性を向上させるべくタグリーダから短期間の間に連続して複数回 R F I D 送信要求が送られてくることを想定したものであり、その場合毎回ランダムに生成された偽 R F I D を発信したのでは、適正な R F I D として読取ってくれない不都合が生じる。そこで、前回の R F I D 発信から 5 秒経過していない時には、前回と同じコードの R F I D を発信するようにし、偽 R F I D であることが見破られる不都合を防止できるようにしている。また、タグリーダの読取り信頼性を向上させる目的ではなく、受信した R F I D が本物の R F I D であるかまたは偽物の R F I D であるかを見極めるために連続して複数回 R F I D 送信要求を発信するタグリーダが設置される可能性も予測される。そのようなタイプのタグリーダが設置されたとしても、所定期間内（例えば 5 秒間）の範囲内で再度 R F I D 発信要求が行われてくれば、前回と同じコードの R F I D を送り返すために、偽 R F I D であることが見破られる不都合を防止できる。この場合、第 1 回目の偽 R F I D を送信した後一旦電源用電波が停止され、その後（例えば 5 秒後）再度電源用電波が発信されて R F I D 発信要求が行われたとしても、コンデンサ 1 1 0 からの供給電力により R F I D タグ 1 a が作動中であるため、前回と同じ偽 R F I D を再発信することができる。

【 0 2 4 2 】

前回の R F I D の発信から 5 秒経過している場合には S G 3 a により Y E S の判断がなされて S G 5 へ進み、偽 R F I D が E E P R O M 1 9 4 に記憶されているか否かの判断がなされる。記憶されている場合には、S G 9 へ進み、その記憶している偽 R F I D の内前回発信した R F I D の次の順番の R F I D を発信する処理がなされる。一方、偽 R F I D の記憶がない場合には、S G 6 へ進み、個数決定用乱数 K R を生成して R F I D の送信個数を決定する処理がなされ、S G 7 により、その決定された個数だけの R F I D のコードを決定するための乱数 I D R を生成して偽 R F I D の各コードを決定して発信する処理が

なされる。そして、SG8により、その決定された偽RFIDをそれぞれEEPROM194に記憶させる処理がなされる。

【0243】

ブラウザフォン30がトラップモードとなっている場合には、SG4により、YESの判断がなされてSG10へ進み、業社の店名を受信しているか否かの判断がなされる。後述する自動決済処理等の場合には、販売業者の店名信号を受信する（SH2参照）。業社の店名を受信しておれば、制御がSG11へ進み、受信した業社に対応するトラップ型RFIDがVP用IC端末19Vに記憶されているか否かの判断がなされる（図8、図9参照）。記憶されている場合にはSG12へ進み、その受信し業社に対応するトラップ型RFIDを発信する処理がなされる。一方、SG10またはSG12によりNOの判断がなされた場合には制御がSG13へ進み、図28のSF7bにより予め選択指定されている業者に対応するRFIDをVP用IC端末19VのEEPROM26から読出して（図8、図9参照）、そのトラップ型RFIDを発信する処理がなされる。例えば、個人ユーザがポイントカードの発行を行っていないスーパーマーケット等の業社内を歩いたりその業社内で購入商品を自動決済した場合等においてその業社側からRFID送信要求が発信された場合には、SF7bにより予め選択指定されている業者に対応するトラップ型RFIDが発信されることとなる。例えば、個人ユーザがMTTの業社を選択操作してSF7bによりその選択指定された業者MTTをブラウザフォン30に記憶させた場合において、ポイントカードを新規発行していないすなわちVPを登録していないスーパーマーケット（RIFに）においてRFID送信要求が出された場合には、ブラウザフォン30からMTTに対応するトラップ型RFIDであるmttが発信されることとなる。そのトラップ型RFIDであるmttを発信した後、スーパーマーケットRIFがトラップ型VPであるE（B13P）宛にダイレクトメールあるいはEメールが送信されてきた場合には（図9参照）、業社MTTに登録されているトラップ型VPの個人情報E（B13P）、Eメールアドレス△△△△△等が、業社MTTからスーパーマーケットRIFに不正に横流しことが分かる。このように、トラップ型RFIDを発信することにより、後日送られてきた電子メールやダイレクトメールの宛名と送り主とをチェックすることにより、個人情報が不正に横流しされたか否かをチェックすることが可能となる。

【0244】

図30は、個人ユーザが百貨店等の業社において商品を購入した後自動決済を行なう場合の決済用ゲートの通過状態を示す説明図である。百貨店（業社）206により個人ユーザ202が商品を購入して手提げ袋203に詰め込み、決済用の通過ゲート206を通過して購入商品の決済を行なう。購入商品には、それぞれにRFIDタグが付されており、通過ゲート206に設けられているタグリーダーライタ201との間で交信を行なう。また、個人ユーザ202はブラウザフォン30を所持している。

【0245】

百貨店（業社）206には、決済サーバ204とデータベース205とが設置されている。決済サーバ204は、通過ゲート206に設けられているタグリーダーライタ201と電氣的に接続されている。タグリーダーライタ201は、通過ゲート206を通過する際に個人ユーザ202の所持しているブラウザフォン30および個人ユーザ202の手提げ袋203内に収納されている購入商品に付されているRFIDタグと交信を行ない、決済に必要なデータを決済サーバ204へ送信する。決済サーバ204に接続されているデータベース205には、顧客データが記憶されている。具体的には、顧客名E（B13P）、E（NPXA）…と、それら各顧客名に対応するポイント数、住所、Eメールアドレスが記憶されている。住所は、トラップ型VPであるE（B13P）のコンビニエンスストアの住所□×○、E（NPXA）のコンビニエンスストアの住所である△○○（図3参照）であり、Eメールアドレスは、トラップ型VPの場合には金融機関7に開設しているトラップ型VP用のEメールアドレスである△△△△△となっている（図3参照）。なお、購入商品に付されているRFIDタグは、決済用ゲートを通過して決済が完了し時点でタグリーダーライタ201からの所定の信号（たとえば決済完了信号）を受信した初めてRFI

D発信停止状態にすることが可能となる。したがって、決済完了前においては、S D 7、S F 5等に従ってブラウザフォン30からOFFモード指令が発信されたとしてもRFID発信停止状態にはならない。

【0246】

図31は、図14のS100に示された自動決済処理のサブルーチンプログラムを示すフローチャートである。SH1により、自動決済開始信号を受信したか否かの判断がなされる。個人ユーザ202が通過ゲート206を通過する際にタグリーダーライタ201から自動決済開始信号がブラウザフォン30に送信されて来れば、SH1によりYESの判断がなされてSH2へ進み、販売業社である百貨店206の店名信号を受信したか否かの判断がなされ、受信するまで待機する。タグリーダーライタ201から店名信号がブラウザフォン30へ送信されて来れば、SH3へ進み、送信されてきた店名(業社名)に対応するトラップ型RFIDがVP用IC端末19Vに既に記憶されているか否かの判断がなされる。既に記憶されている場合にはSH5へ進み、まだ記憶されていない場合にはSH4へ進み、送信されて来た店名(業社名)に対応させて新しいトラップ型RFIDを生成してVP用IC端末19VをEEPROM26に記憶させる処理がなされる。

【0247】

次にSH5へ進み、送信されてきた店名の業社がポイントカードを発行して登録している業社であるか否かの判断がなされる。ポイントカードの登録がなされていない場合にはSH14へ進むが、ポイントカードの発行がなされている業社の場合にはSH6へ進み、デビット決済、クレジットカード決済の両方が可能な旨をブラウザフォン30により表示する処理がなされる。

【0248】

SH1～SH6の処理の間に、タグリーダーライタ201は手提げ袋203に収納されている各購入商品に付されているRFIDタグと交信してそのRFIDタグから送信されてきた各RFIDを決済サーバ204へ送信する。決済サーバ204は、その送信されてきた各RFIDに対応する商品価格を割出してその合計を算出してタグリーダーライタ201へ送信する。タグリーダーライタ201は、その合計金額を個人ユーザ203のブラウザフォン30へ送信する。

【0249】

次に制御はSH7へ進み、払出金額を受信する処理がなされる。タグリーダーライタ201から合計金額(払出金額)がブラウザフォン30へ送信されてくることにより、この支払金額の受信処理が行なわれる。次にSH8へ進み、決済処理の入力操作があったか否かの判断がなされる。個人ユーザ202がブラウザフォン30により決済処理を入力する。決済の種類は、前述したデビットカード決済とクレジットカード決済とリロード金額決済とがある。リロード金額決済とは、個人ユーザ202の銀行口座の残額から一部ブラウザフォン30に引き落としてブラウザフォン30にリロードした金額を用いて決済を行なうものである。次にSH9へ進み、SH7により受信された支払金額をブラウザフォン30により表示する処理がなされる。次にSH10へ進み、その支払い金額に同意して決済を行なうためのOK操作があったか否かの判断がなされる。OK操作がない場合にはSH11へ進み、決済をキャンセルするキャンセル操作があったか否かの判断がなされ、ない場合にはSH10へ戻る。このSH10、SH11のループの巡回途中で、顧客202がブラウザフォン30を操作してOK操作を入力すれば制御がSH13へ進む。一方、個人ユーザ202がキャンセル操作を行えばSH12へ進み、ブラウザフォン30からタグリーダーライタ201へキャンセル信号が発信され、商品の購入をキャンセルする意思表示が送信される。

【0250】

SH13では、SG8により入力された決済の種類がリロード金額決済であるか否かの判断がなされる。リロード金額決済の場合にはSH14へ進み、SH7により受信した支払金額をブラウザフォン30にリロードされているリロード金額との大小関係を判別し、支払金額以上のリロード金額があるか否かの判断がなされる。支払金額以上のリロード金

額がある場合にはSH15によりOK信号がブラウザフォン30からタグリーダライタ201へ送信され、その信号が決済サーバ204へ送信される。次にSH16により、VP用決済処理がなされる。このVP用決済処理は、図53～図55にその詳細が示されている。SH16の場合にはリロード金額決済を行なうために、図55のS249によりYESの判断がなされてS250～S252bの処理が行なわれることとなる。

【0251】

次にSH17により、ポイントカード加算処理が行なわれる。このポイントカード加算処理は、購入商品の合計金額に対応するポイント数をポイントカードに加算するための処理であり、図32(a)に示されている。

【0252】

一方、SH14によりNOの判断がなされた場合には、SH18へ進み、キャンセル信号をブラウザフォン30からタグリーダライタ201へ送信する処理がなされ、その信号が決済サーバ204へ送信される。次にSH19へ進み、残額不足である旨の表示がブラウザフォン30により行なわれる。

【0253】

なお、決済相手の業社がポイントカードを登録していない業社の場合にはSH5によりNOの判断がなされてSH14～SH19のリロード決済の処理が行なわれることとなり、クレジット決済やデビット決済は行なわれない。これは、ポイントカードを登録していない業社の場合には個人ユーザ202のVP情報をその業社に登録していないために、VPとしてクレジット決済やデビット決済を行なうことが不可能なためである。

【0254】

SH13によりNOの判断がなされた場合にはSH20へ進み、入力された決済処理がクレジット決済であるか否かの判断がなされる。クレジット決済の場合にはSH22に進み、OK信号がブラウザフォン30からタグリーダライタ201へ送信され、その信号が決済サーバ204へ送信される。次に、SH23へ進み、VP用決済処理が行われる。このSH23のVP用決済処理は、クレジット決済であるために、図55のS238によりYESの判断がなされてS237～S248のクレジット決済処理が行なわれることとなる。

【0255】

入力された決済処理がデビット決済の場合にはSH20によりNOの判断がなされてSH21へ進み、デビット決済要求信号をブラウザフォン30がタグリーダライタ201へ送信し、その信号が決済サーバ204へ送信される。決済サーバ204は、データベース200を検索して決済相手の顧客名に対応するバーチャル口座番号例えばE(2503)を割出し(図30参照)、そのバーチャル口座番号内に残額がどの程度あるかを金融機関7に問い合わせる。そして、残額が支払金額以上の場合には、OK信号をタグリーダライタ201を介してブラウザフォン30へ送信する。一方、残額が支払金額未満であった場合には、NG信号をタグリーダライタ201を介してブラウザフォン30へ送信する。

【0256】

ブラウザフォン30では、SH24により、OK信号を受信したか否かの判断がなされ、未だに受信していない場合にはSH26によりNG信号を受信したか否かの判断がなされ、未だに受信していない場合にはSH24へ戻る。

【0257】

SH24、SH26のループの巡回途中で、タグリーダライタ201からOK信号がブラウザフォン30へ送信されてくれば、制御がSH25へ進み、VP用決済処理がなされる。この場合には、デビット決済であるために、図54(b)のS220によりYESの判断がなされてS235～S234のデビット決済処理が行なわれることとなる。

【0258】

タグリーダライタ201からNG信号がブラウザフォン30へ送信されてくれば、SH26によりYESの判断がなされてSH27へ進み、NG表示がブラウザフォン30により行なわれる。

【 0 2 5 9 】

図 3 2 (a) は、S H 1 7 に示されたポイントカード加算処理のサブルーチンプログラムを示すフローチャートである。S I 1 により、該当する V P 情報を発信する処理が行なわれる。これは、決済相手の業社に登録されている V P を V P 用 I C 端末 1 9 V の E E P R O M 2 6 から検索し、その検索された V P 氏名等の情報（例えば E (B 1 3 P) ）をタグリーダーライタ 2 0 1 へ送信する。タグリーダーライタ 2 0 1 は、その受信した V P 情報を決済サーバ 2 0 4 へ送信する。決済サーバ 2 0 4 は、受信した V P 氏名に基づいてデータベース 2 0 5 を検索し（図 3 0 参照）、例えば受信した顧客名が E (B 1 3 P) の場合には、現在のポイント数 1 9 0 1 8 を割出して、その現在のポイント数に対し、購入商品の合計金額に対応したポイント数を加算する処理を行なう。そしてその加算ポイント数を決済サーバ 2 0 4 がタグリーダーライタ 2 0 1 を介してブラウザフォン 3 0 へ送信する。 10

【 0 2 6 0 】

ブラウザフォン 3 0 では、S I 2 によりポイント受信したか否かの判断がなされ、あるまで待機する。そして、タグリーダーライタ 2 0 1 から加算ポイント数を受信すれば、制御が S I 3 へ進み、該当する業社（決済相手の業社）に対応させて V P 用 I C 端末 1 9 V の E E P R O M 2 6 に記憶させる処理が行なわれる。

【 0 2 6 1 】

図 2 3 (b) は、百貨店等の業社 2 0 6 においてポイントカードを新規発行して登録してもらう際のブラウザフォン 3 0 の処理動作を示すフローチャートである。S J 1 により、個人ユーザ 2 0 2 がポイントカード登録操作をブラウザフォン 3 0 により行なったか否かの判断がなされ、行なった場合には S J 2 へ進み、金融機関 7 に既に登録されているトラップ型 V P であって未だポイントカード登録に用いられていないトラップ型 V P は V P 用 I C 端末 1 9 V の E E P R O M 2 6 に記憶されているか否かの判断がなされる。判断の答えが N O の場合には S J 3 へ進み、トラップ型 V P が無い旨の表示がブラウザフォン 3 0 により行なわれる。その際には、個人ユーザ 2 0 2 は、金融機関 7 に対して、新たなトラップ型 V P を生成して登録してもらうための処理を行なう。新たなトラップ型 V P の生成要求があった場合には、金融機関 7 の V P 管理サーバ 9 は、図 3 7 または図 4 0 (b) のトラップ型 V P 処理を行なって新たなトラップ型 V P を生成して登録する処理を行なう。 20

【 0 2 6 2 】

一方、S J 2 により常に登録されているトラップ型 V P であってポイントカードの登録にまだ用いられていないトラップ型 V P の記憶があると判断された場合には、S J 4 へ進み、そのトラップ型 V P の中から 1 つ選択してその住所、氏名等の必要な情報をブラウザフォン 3 0 からタグリーダーライタ 2 0 1 を介して決済サーバ 2 0 4 へ送信する処理が行なわれる。決済サーバ 2 0 4 は、受信したトラップ型 V P 情報に基づいてポイントカードの新規登録を行なっているか否かの判断を行ない、その判断結果をタグリーダーライタ 2 0 1 を介してブラウザフォン 3 0 へ返信する。 30

【 0 2 6 3 】

ブラウザフォン 3 0 では、S J 5 により、O K 信号を受信したか否かの判断を行ない、未だ受信していない場合には S J 6 により N G 信号を受信したか否かの判断を行ない、未だ受信していない場合には S J 5 へ戻る。この S J 5、S J 6 のループの巡回途中で、決済サーバ 2 0 4 の判断結果として O K 信号を受信すれば、S J 5 により Y E S の判断がなされて S J 7 へ進み、ポイントカードの登録相手である業社名を受信したか否かの判断がなされる。決済サーバ 2 0 4 は、O K 信号を送信した後、当店の業社名をタグリーダーライタ 2 0 1 を介してブラウザフォン 3 0 へ送信する。すると、S J 7 により Y E S の判断がなされて S J 8 へ進み、その受信した業社名に対応させてトラップ型 V P を V P 用 I C 端末 1 9 V の E E P R O M 2 6 へ記憶させる処理がなされる。 40

【 0 2 6 4 】

一方、決済サーバ 2 0 4 からの判断結果が N G であった場合には、S J 6 により Y E S の判断がなされて S J 9 へ進み、N G 表示がブラウザフォン 3 0 により行なわれる。 50

【 0 2 6 5 】

図 3 3 は、販売業社 2 0 6 の決済サーバ 2 0 4 の決済処理を示すフローチャートである。S K 1 により、自動決済の開始であるか否かの判断がなされ、自動決済の開始でない場合には S K 2 に進み、ポイントカードの新規登録要求であるか否かの判断がなされ、新規登録要求でない場合には S K 3 へ進み、その他の処理が行なわれて S K 1 へ戻る。

【 0 2 6 6 】

個人ユーザ 2 0 2 が決済のために通過ゲート 2 0 6 を通過した場合には、S K 1 により Y E S の判断がなされて S K 4 へ進み、店名（業社名）の信号を決済サーバ 2 0 4 がタグリーダライタ 2 0 1 を介してブラウザフォン 3 0 へ送信する指令処理を行なう。次に S K 5 へ進み、R F I D 送信要求の信号をタグリーダライタ 2 0 1 に発信させるための指令処理を行なう。次に S K 6 へ進み、R F I D を受信したか否かの判断がなされ、受信するまで待機する。手提げ袋 2 0 3 に収納されている各購入商品に付されている R F I D タグから発信された各 R F I D がタグリーダライタ 2 0 1 に読取られてその信号が決済サーバ 2 0 4 へ送信される。すると、S K 6 により Y E S の判断がなされて S K 7 へ進み、受信した各 R F I D の内当店の販売商品として登録されている R F I D を検索する処理がなされる。百貨店（業社）2 0 6 のデータベース 2 0 5 には、図 3 1 に示した顧客データばかりでなく、販売商品の各 R F I D とそれに対応させた商品価格データが記憶されている。決済サーバ 2 0 4 は、データベース 2 0 5 を検索して、データベース 2 0 5 に登録されている R F I D 中に送信されてきた R F I D と一致するものであるか否かを判別し、一致するものを検索する。そして S K 8 により、その一致する R F I D の商品価格の合計を算出する処理がなされる。次に、S K 9 へ進み、その算出した合計金額を支払い金額としてタグリーダライタ 2 0 1 を介してブラウザフォン 3 0 へ送信する処理が行なわれる。

【 0 2 6 7 】

次に S K 1 0 へ進み、ブラウザフォン 3 0 から O K 信号を受信したか否かの判断がなされ、また S K 1 1 により、ブラウザフォン 3 0 からキャンセル信号を受信したか否かの判断がなされる。この S K 1 0、S K 1 1 のループの巡回途中で、ブラウザフォン 3 0 から O K 信号が送信されてくれば S K 1 2 により決済処理を行なう。この決済処理は、図 5 3 ~ 図 5 5 のブラウザフォン 3 0 側の決済処理動作に対応した販売業者側の決済サーバ 2 0 4 の処理動作である。次に S K 1 3 へ進み、販売された商品の R F I D をデータベース 2 0 5 の登録から抹消する処理がなされる。次に S K 1 4 へ進み、販売商品の合計金額に対応する加算ポイント数を算出する処理がなされる。

【 0 2 6 8 】

S K 1 5 へ進み、V P 情報を受信したか否かの判断がなされ、受信するまで待機する。S I 1 に従ってブラウザフォン 3 0 から該当する V P 情報が送信されてくれば、制御が S K 1 6 へ進み、加算ポイント数をタグリーダライタ 2 0 1 からブラウザフォン 3 0 へ送信する処理がなされる。次に S K 1 7 へ進み、受信した V P に対応するポイントデータをデータベース 2 0 5 から割出し（図 3 0 参照）、その割出されたポイント数に対し加算ポイント数を加算更新する処理がなされて S K 1 へ戻る。

【 0 2 6 9 】

次に、ポイントカードの新規登録要求があった場合には S K 2 により Y E S の判断がなされて S K 2 1 へ進み、V P を受信したか否かの判断がなされ、受信するまで待機する。S J 4 に従ってブラウザフォン 3 0 からトラップ型 V P 情報が送信されてくれば、制御が S K 2 2 へ進み、金融機関 7 の V P 管理サーバ 9 に適正に登録されている V P であるか否かの問合せ処理がなされる。V P 管理サーバ 9 では、データベース 1 2 a に適正に登録されている V P であるか否かをチェックし、そのチェック結果を販売業者 2 0 6 の決済サーバ 2 0 4 へ返信する。決済サーバ 2 0 4 では、返信されてきたチェック結果が適正であるか否か S K 2 3 により判定し、適正でない場合には S K 2 4 により N G をタグリーダライタ 2 0 1 を介してブラウザフォン 3 0 へ返信する処理がなされる。一方、適正である場合には S K 1 8 へ進み、O K 信号をタグリーダライタ 2 0 1 を介してブラウザフォン 3 0 へ返信する処理がなされる。

【 0 2 7 0 】

S K 1 9 へ進み、店名（業社名）をタグリーダーライタ 2 0 1 を介してブラウザフォン 3 0 へ送信する処理がなされ、S K 2 2 により、ポイント対象顧客として V P をデータベース 2 0 5 に新規登録する処理がなされる（図 3 0 参照）。

【 0 2 7 1 】

次に、V P 用 I C 端末 1 9 V の制御動作を図 3 4 に基づいて説明する。V P 用 I C 端末 1 9 V は、S 2 5 3 により、暗証番号チェック処理を行なう。次に S 2 5 4 へ進み、トラップ型 R F I D 処理を行なう。次に S 2 5 5 へ進み、本人証明処理を行なう。次に S 2 5 6 へ進み、データ入力処理を行なう。次に S 2 5 7 へ進み、ユーザエージェント動作処理を行なう。次に S 2 5 8 へ進み、リロード金額の使用処理を行なう。次に S 2 5 9 へ進み、署名処理を行なう。次に S 6 1 5 により、トラップ型 V P 処理がなされる。この処理は、図 3 7 に基づいて後述する。 10

【 0 2 7 2 】

図 3 5 (a) は、S 2 5 3 に示された暗証番号チェック処理のサブルーチンプログラムを示すフローチャートである。S 2 6 8 により、暗証番号が入力されたか否かの判断がなされ、入力されていない場合にはこのままサブルーチンプログラムが終了する。一方、暗証番号が入力されれば、S 2 6 9 へ進み、入力された暗証番号を記憶している暗証番号と照合する処理がなされる。次に S 2 7 0 へ進み、照合の結果一致するか否かの判断がなされ、一致しない場合には S 2 7 1 へ進み、不適正な旨をブラウザフォン 3 0 へ送信する処理がなされる。一方、一致する場合には S 2 7 2 へ進み、適正な旨の返信を行なう。 20

【 0 2 7 3 】

図 3 5 (b) は、S 2 5 4 に示されたトラップ型 R F I D 処理（V P 用）のサブルーチンプログラムを示すフローチャートである。S 2 7 3 により、業社名の入力があるか否かの判断がなされる。ブラウザフォン 3 0 は V P 用 I C 端末 1 9 V にトラップ型 R F I D に対応する業社名（店名）を入力する（S G 1 1、S G 1 3、S H 3）。入力があれば S 2 7 4 へ進み、入力された業社名に対応するトラップ型 R F I D の読出し要求か否かが判断される。S G 1 1、S G 1 3 にしたがった要求の場合には S 2 7 4 により Y E S の判断がなされ、S 2 7 5 により、E E P R O M 2 6 に記憶されているトラップ型 R F I D の中から入力された業社名に対応するトラップ型 R F I D を検索する処理がなされる。検索の結果対応するトラップ型 R F I D が記憶されているか否かが S 2 7 6 により判断される。記憶がある場合にはその対応するトラップ型 R F I D をブラウザフォン 3 0 へ出力する処理が S 2 7 7 によりなされる。一方、S 2 7 6 により対応するトラップ型 R F I D の記憶がないと判断された場合には、ブラウザフォン 3 0 へ出力する処理がなされる。 30

【 0 2 7 4 】

ブラウザフォン 3 0 は、記憶がない旨の信号を受信した場合には、S H 3 により N O の判断を行ない、S H 4 により、業社名に対応させてトラップ型 R F I D を記憶させる指令を V P 用 I C 端末 1 9 V へ出力する。それを受けた V P 用 I C 端末 1 9 V は、S 2 7 3 により Y E S S 2 7 4 により N O の判断を行い、S 2 7 8 により、新たなトラップ型 R F I D を生成して、業社名に対応させて E E P R O M 2 6 に記憶する処理を行なう。

【 0 2 7 5 】

図 3 5 (c) は、S 2 5 5 に示された本人証明処理（V P 用）のサブルーチンプログラムを示すフローチャートである。S 2 8 0 により、乱数 R の入力があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。乱数 R の入力があった場合に S 2 8 1 へ進み、V P 出生依頼時であるか否かの判断がなされる。V P 出生依頼時の場合には、S 6、S 1 5 1 で説明したように、R P の認証鍵 K N を用いて R P が正当な本人であることを証明する必要がある。そのために、V P 出生依頼時の場合には S 2 8 3 進み、入力された乱数 R を R P の認証鍵 K N で暗号化して I を生成する処理すなわち $I = E_{K_N}(R)$ の算出処理を行なう。そして、S 2 8 4 により、その算出された I をブラウザフォン 3 0 へ出力する処理がなされる。

【 0 2 7 6 】

一方、VP出生依頼時でない場合には、S281によりNOの判断がなされてS282へ進み、VPは正当な本人であることを証明するべく、VPの秘密鍵KSを用いて入力された乱数Rを暗号化してIを算出する処理、すなわち、 $I = E_{KS}(R)$ を算出する処理を行なう。そしてS248により、その算出されたIをブラウザフォン30へ出力する処理がなされる。

【0277】

図36(a)は、S256、S263に示されたデータ入力処理のサブルーチンプログラムを示すフローチャートである。S293により、データ入力があったか否かの判断がなされる。入力されるデータとしては、前述したように、VP管理サーバ9によって誕生したVPに関するデータが記録されているCD-ROMの記録データ、ユーザエージェントの知識データ(S179、S189参照)、引落し額G(S181、S191参照)等がある。これらのデータが入力されれば、制御がS294へ進み、入力データに対応する記憶領域に入力データを記憶させる処理がなされる。

【0278】

図36(b)は、S257、S264に示されたユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートである。S295により、公開鍵出力要求があったか否かの判断がなされる。公開鍵の出力要求があった場合には、S298に進み、記憶している公開鍵KPを出力する処理がなされる。S295によりNOの判断がなされた場合にS296へ進み、デビットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS299へ進み、記憶しているデビットカード情報を出力する処理がなされる。

【0279】

S296によりNOの判断がなされた場合にはS297へ進み、クレジットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS300へ進み、記憶しているクレジットカード情報を出力する処理がなされる。次にS301へ進み、その他の動作処理が行なわれる。このその他の動作処理は、図30に基づいて後述する。

【0280】

図36(c)は、S258、S265に示されたリロード金額の使用処理のサブルーチンプログラムを示すフローチャートである。S302により、引落し額Gの引落し要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には、S303へ進み、記憶しているリロード金額がGを減算する処理がなされ、S304へ進み、引落し完了信号を返信する処理がなされる。

【0281】

図36(d)は、S259により示されたVP署名処理のサブルーチンプログラムを示すフローチャートである。S999により、メッセージダイジェストMDとVP氏名との入力ブラウザフォン30からあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【0282】

MDとVP氏名との入力があった場合には制御がS998へ進み、その入力されたVP氏名から秘密鍵(KS)を生成する処理がなされる。具体的には、VP用IC端末19Vは、入力されたVP氏名に基づいてトラップ型RFIDデータ記憶領域を検索してその入力されたVP氏名が本名B13P(図9参照)を何回暗号化したものであるかを割出す。その割出された暗号化回数だけVPの秘密鍵をVPの秘密鍵で暗号化して秘密鍵(KS)を生成する。

【0283】

次に制御がS997へ進み、その秘密鍵(KS)を用いてメッセージダイジェストMDを復号化して二重署名を生成する処理がなされる。次に制御がS998へ進み、その二重署名 $D_{(KS)}(MD)$ をブラウザフォン30へ出力する処理がなされる。

【0284】

図37は、S615により示されたトラップ型VP処理のサブルーチンプログラムを示

すフローチャートである。S 6 2 0により、新たなトラップ型 V P の生成要求があったか否かの判断がなされ、ない場合には S 6 2 3 へ進み、トラップ型 V P が使用済みであるか否かの問合せがあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【 0 2 8 5 】

ブラウザフォン 3 0 が S 5 9 8 に従って V P 用 I C 端末 1 9 V に新たなトラップ型 V P の生成要求を出した場合には、S 6 2 0 により Y E S の判断がなされて制御が S 6 2 1 へ進む。S 6 2 1 では、V P 用 I C 端末 1 9 V のトラップ型 R F I D データ領域の最後の V P 氏名の暗号回数 n を「1」加算して、V P の本名を n + 1 回秘密鍵で暗号化して新たなトラップ型 V P 氏名を生成する処理がなされる。たとえば図 9 の場合には、トラップ型 R F I D データ領域の最後の V P 氏名 E³ (B 1 3 P) の暗号回数が 3 回であり、これに「1」加算して暗号回数 4 にし、V P の本名 B 1 3 P を 4 回暗号化して新たなトラップ型 V P 氏名 E⁴ (B 1 3 P) を生成する処理がなされる。

【 0 2 8 6 】

次に S 6 2 2 へ進み、その生成されたトラップ型 V P を、ブラウザフォン 3 0 へ出力するとともに、トラップ型 R F I D 領域における最後の V P 氏名の次の空き領域に記憶させる処理がなされる。

【 0 2 8 7 】

S 5 9 0 に従ってブラウザフォン 3 0 が V P 用 I C 端末 1 9 V に対し今アクセスしようとしているサイト (図 3 0 の自動決済しようとしている業社) にトラップ型 V P が既に使用されているか否かの問合せを行なった場合には、S 6 2 3 により Y E S の判断がなされて制御が S 6 2 4 へ進む。この問合せの際にはブラウザフォン 3 0 は V P 用 I C 端末 1 9 V に対し、今アクセスしようとしているサイト名 (図 3 0 の自動決済しようとしている業社名) も併せて伝送する。S 6 2 4 では、トラップ型 R F I D 領域 (図 9 参照) を検索する処理がなされる。制御が S 6 2 5 へ進み、伝送されてきたサイト名 (業社名) に対しトラップ型 V P 氏名が使用済みであるか否かの判断がなされる。たとえばブラウザフォン 3 0 から伝送されてきたサイト名 (業社名) が M E C であった場合には、図 9 を参照して、トラップ型 V P 氏名 E² (B 1 3 P) が使用済みであることがわかる。

【 0 2 8 8 】

トラップ型 V P 氏名が使用済みであると判断された場合には制御が S 6 2 6 へ進み、使用済みである旨をブラウザフォン 3 0 へ出力するとともに、S 6 2 7 により、使用されているトラップ型 V P とそれに対応するトラップ型 R F I D データとをブラウザフォン 3 0 へ出力する処理がなされる。たとえば、図 9 の場合には、伝送されてきたサイト名 (業社名) が M E C であった場合には、トラップ型 V P として E² (B 1 3 P) がブラウザフォン 3 0 へ出力されるとともに、トラップ型 R F I D データ m e c がブラウザフォン 3 0 へ出力される。

【 0 2 8 9 】

図 9 のトラップ型 R F I D 領域を検索した結果、ブラウザフォン 3 0 から伝送されてきたサイト名 (業社名) に対しトラップ型 V P が未だ使用されていない場合には S 6 2 5 により N O の判断がなされて制御が S 6 2 8 へ進み、未使用の旨をブラウザフォン 3 0 へ出力する処理がなされる。

【 0 2 9 0 】

図 3 8、図 3 9 は、コンビニエンスストア 2 のサーバ 1 6 の処理動作を説明するためのフローチャートである。S 3 1 5 により、V P の氏名、E メールアドレス、金融機関の名称を受信したか否かの判断がなされ、受信していない場合に S 3 1 6 へ進み、V P が購入した商品を預かったか否かの判断がなされ、預かっていない場合に S 3 1 7 へ進み、商品の引取り操作があったか否かの判断がなされ、ない場合には S 3 1 8 へ進み、その他の処理を行なった後 S 3 1 5 へ戻る。

【 0 2 9 1 】

この S 3 1 5 ~ S 3 1 8 のループの巡回途中で、決済サーバ 1 0 が誕生した V P の氏名

10

20

30

40

50

、Eメールアドレス、当該金融機関の名称をコンビニエンスストア2へ送信した場合には（S18参照）、S315によりYESの判断がなされてS319へ進み、正当機関チェック処理がなされた後、S320へ進む。

【0292】

S320では、 $R = D_k, (L)$ であるか否かの判断がなされ、正当機関でない場合にはNOの判断がなされてS321へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合にはS320によりYESの判断がなされてS322へ進み、受信データをデータベース17へ登録する処理がなされる。

【0293】

ユーザがVPとしてたとえば電子ショッピング等を行なってそのVPの住所であるコンビニエンスストア2に購入商品が配達されてコンビニエンスストア2がその商品を預かった場合には、S316によりYESの判断がなされてS316aへ進み、該当するVPの商品預かり情報のアドレス領域に商品を預かった旨の情報を記憶させる処理がなされる。その際に、当該商品の決済が済んでいるか否かの情報も併せて記憶させる。次に制御がS323へ進み、当該VPのEメールアドレスを割出し、そのEメールアドレスへ商品を預かった旨のメールを送信する処理がなされる。VPは、そのEメールを見ることにより、コンビニエンスストアに購入商品が配達されたことを知ることができ、その商品を引取るためにそのコンビニエンスストアに出向く。

【0294】

ユーザがVPとしてコンビニエンスストア2に出向き、配達された商品を引取るための操作を行なえば、S317によりYESの判断がなされる。そして制御がS324へ進み、VP用IC端末19Vの差込指示が表示される。それを見たユーザは、自己のVP用IC端末19Vを端末73のUSBポートへ差込んで接続する。すると、S325によりYESの判断がなされてS326へ進み、暗証番号チェック処理がなされる。ユーザは、端末73に設けられているキーボードからVP用の暗証番号を入力する。暗証番号が一致して適正であることを条件として、制御がS327へ進み、接続されているVP用IC端末19VからVP用の氏名を呼出してそれに基づいてデータベース17を検索する処理がなされる。そして、該当するVPの商品預かり情報のアドレス領域に、商品預かり情報が記録されているか否かの判断がS328によりなされる。商品預かり情報がなければS329へ進み、預かり商品がない旨が表示される。一方、商品預かり情報がある場合にはS330へ進み、電子証明書の出力要求がVP用IC端末19Vに対しなされる。VP用IC端末19Vは、それを受けて、記憶している電子証明書をサーバ16に出力する。すると、S331によりYESの判断がなされてS332へ進み、出力されてきた電子証明書内の公開鍵KPを読み出し、S333により、本人チェック処理がなされる。

【0295】

差込まれているVP用IC端末19Vは、前述したように、VP本名に対する電子証明書は格納しているものの、トラップ型VPに対する電子証明書は格納しておらず、そのトラップ型VPに対する電子証明書はXMLストア50に格納されている。VP本名を用いて電子ショッピング等を行なってその購入商品がコンビニエンスストア2へ届けられた場合には、S327に従って呼出されたVP氏名はVPの本名となる。その場合には、S330の要求に従ってVP用IC端末19Vは電子証明書を出力することができる。その場合にS331によりYESの判断がなされて制御がS332へ進む。一方、トラップ型VP氏名を用いて電子ショッピングを行ないその購入商品がコンビニエンスストア2へ届けられた場合には、その商品をトラップ型VPとしてコンビニエンスストア2へ引取りに行くこととなる。その場合には、S327によってVP用IC端末19Vから呼出されるVP氏名は、トラップ型VP氏名となる。その結果、そのトラップ型VP氏名に対応する電子証明書の出力要求がS330からVP用IC端末19Vに対し出される。その場合には、VP用IC端末19Vは、XMLストア50から電子証明書を取り寄せる旨の指示を出力する。

【0296】

その出力があれば、制御が S 6 3 1 へ進み、XML ストア 5 0 へアクセスして該当する電子証明書を取り寄せる処理がなされた後制御が S 3 3 2 へ進む。

【 0 2 9 7 】

次に S 3 3 4 へ進み、 $R = D_k(I)$ であるか否かの判断がなされる。正当でないなりすましの VP である場合には、S 3 3 4 により NO の判断がなされて S 3 3 5 へ進み、不適正である旨が表示される。一方、適正な VP であった場合には、制御が S 3 3 6 へ進み、預かり商品番号を表示し、S 3 3 7 により、その商品に関し決済済みであるか否かの判断がなされ、決済済みの場合には S 3 3 9 へ進むが、決済済みでない場合には S 3 3 8 へ進み、決済処理が行なわれる。

【 0 2 9 8 】

S 3 3 9 では、商品の引渡し完了したか否かの判断がなされる。コンビニエンスストア 2 の店員は、S 3 3 6 により表示された預かり商品番号を見て、該当する番号の商品を探し出し、顧客にその商品を引渡しした後、商品引渡し完了操作を行なう。すると、S 3 3 9 により YES の判断がなされて S 3 4 0 へ進み、データベース 1 7 の商品預かり情報のアドレス領域を更新し、商品預かりなしの状態にした後、S 3 1 5 へ戻る。

【 0 2 9 9 】

S 3 2 6 の暗証番号チェック処理は、図 3 9 (a) に示されている。S 3 4 5 により、暗証番号の入力指示が表示され、ユーザが入力すれば S 3 4 7 へ進み、その入力された暗証番号をサーバ 1 6 に接続されている VP 用 IC 端末 1 9 V へ伝送し、その暗証番号の適否の判定結果が VP 用 IC 端末 1 9 V から返送されてくれば、S 3 4 9 へ進む。S 3 4 9 20
では、適正な判定結果か否かが判別され、不適正であれば S 3 5 0 により不適正の表示を行なって S 3 1 5 へ戻るが、適正であればこのサブルーチンが終了して、制御が S 3 2 7 へ進む。

【 0 3 0 0 】

S 3 3 3 の本人チェック処理は、図 3 9 (b) に示されている。S 3 5 5 により、乱数 R を生成して VP 用 IC 端末へ伝送する処理がなされ、チャレンジデータ R に対するレスポンスデータ I が VP 用 IC 端末から返送されてくるまで待機する。I が返送されてくれば、このサブルーチンが終了する。

【 0 3 0 1 】

S 3 3 8 の決済処理は、図 3 9 (c) に示されている。S 3 5 9 により、預かり商品の 30
価格を表示する処理がなされ、S 3 6 0 へ進み、入金があるか否かの判断がなされる。ない場合には S 3 6 2 へ進み、リロード金額による支払操作があったか否かの判断がなされ、ない場合には S 3 6 0 へ戻る。そして、ユーザが現金による支払を行なってコンビニエンスストアの店員が入金があった旨の操作を行なえば、S 3 6 0 により YES の判断がなされて S 3 6 1 へ進み、商品販売会社の口座へ入金処理を行なってこのサブルーチンプログラムが終了する。

【 0 3 0 2 】

一方、ユーザが VP 用 IC 端末 1 9 に記憶されているリロード金額を使用して支払操作を行なうべくその旨の操作がなされれば、S 3 6 2 により YES の判断がなされて S 3 6 3 へ進み、価格 G の引落し要求を VP 用 IC 端末 1 9 V へ伝送する処理がなされる。そして 40
S 3 6 4 へ進み、VP 用 IC 端末 1 9 V から引落し完了信号が出力されてきたか否かの判断がなされ、出力されてくるまで待機する。そして、引落し完了信号を受信すれば、S 3 6 4 により YES の判断がなされて S 3 6 1 へ進む。

【 0 3 0 3 】

次に、別実施の形態を説明する。この別実施の形態は、ブラウザフォン 3 0 やユーザのパーソナルコンピュータ等のユーザ側端末および IC 端末 1 9 および Web サイト (業社) によって、個人情報保護のシステムが完結する簡易型システムである。前述した実施の形態との相違は、トラップ型 VP の E メールアドレスが VP 本名の E メールアドレスと同じである。よって、トラップ型 VP 宛の E メールを金融機関 7 が転送する必要がない。またトラップ型 VP の氏名は、そのトラップ型 VP がアクセスするサイト (業社) の名称を 50

、VP本名に用いられる秘密鍵で暗号化したものを用いる。トラップ型VPの口座番号やクレジット番号も、VPが本名として用いる口座番号、クレジット番号と同じものを用いる。

【 0 3 0 4 】

図40(a)は、VP用IC端末19VのEEPROM26のトラップ型RFID領域に格納されている情報を示す図である。このトラップ型RFID領域には、VP氏名として、VPの本名B13Pのみが記憶され、トラップ型VP氏名は何ら記憶されない。トラップ型VPの氏名は、トラップ型VPとしてアクセスしたサイト(業社)を本名のVPの秘密鍵KSBで暗号化したものを用いる。この暗号化回数は1回に限らず2回以上の或る定められた回数であってもよい。よって、トラップ型VPがアクセスしたサイト名(業社名)のみを記憶させることにより、そのサイト名(業社名)に対応するトラップ型VPの氏名は、わざわざ記憶させなくとも、 $E_{K_{SB}}$ (業社名)の演算式に従って必要に応じてその都度算出することができる。トラップ型VPの秘密鍵は、トラップ型VPに対応するサイト名(業社名)を本名のVPの秘密鍵KSBで復号化したものを用いる。よって、トラップ型VPに対応させて逐一公開鍵や秘密鍵をVP用IC端末19Vに記憶させる必要はなく、秘密鍵= $D_{K_{SB}}$ (業社名)の演算式に従って必要に応じてその都度算出することができる。よって、XMLストア50の「暗号回数」の記憶が不要となる。

【 0 3 0 5 】

図40(b)は、トラップ型VP処理のサブルーチンプログラムを示すフローチャートである。このサブルーチンプログラムは、図37に示したトラップ型VP処理の別実施の形態である。S960により、新たなトラップ型VPの生成要求がブラウザフォン30からあったか否かの判断がなされ、あった場合には制御がS959へ進み、アクセスするサイト(業社名)の名称の入力要求がブラウザフォン30へ出される。ブラウザフォン30からアクセスするサイト(業社)の名称が伝送されてくれば、制御がS957へ進み、その伝送されてきたサイト名(業社名)をVPの本名B13Pの秘密鍵KSBで暗号化して、新たなトラップ型VP氏名である $E_{K_{SB}}$ (業社名)を算出する処理がなされる。次に制御がS956へ進み、その算出した新たなトラップ型VP氏名をブラウザフォン30へ出力する処理がなされ、S954により、入力されたサイト名(業社名)をトラップ型RFID領域に記憶させる処理がなされる。

【 0 3 0 6 】

S953～S948は、図37に示したS623～S628と同じ制御のために、説明の繰返しを省略する。

【 0 3 0 7 】

図40(c)は、VP用IC端末19Vによって行なわれる個人情報流通チェックのサブルーチンプログラムを示すフローチャートである。S970により、Eメールの受信があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。トラップ型VP宛のEメールの受信があれば、ブラウザフォン30は、そのEメールデータをVP用IC端末へ入力する。すると制御がS969へ進み、その入力されたEメールの宛名をVPの本名に用いられる公開鍵KPBで復号化する $D_{K_{PB}}$ (宛名)の演算を行ない、その演算結果がEメールの送信者名と一致するか否かの判断がなされる。

【 0 3 0 8 】

Eメールの宛名はトラップ型VP氏名となっており、そのトラップ型VP氏名は、そのトラップ型VPがアクセスしたサイト名(業社名)をVPの秘密鍵KSBで暗号化したものを用いている。よって、トラップ型VPがその氏名を用いてアクセスしたサイト(業社)からそのトラップ型VP宛にEメールが送信された場合には、S969によりYESの判断がなされる筈である。その場合には、S968により、適正である旨がブラウザフォン30へ出力され、ブラウザフォン30の表示部76によりその旨が表示される。一方、トラップ型VPがその氏名を用いてアクセスしたサイト(業社)以外のサイト(業社)からそのトラップ型VP氏名をEメールの宛名としてEメールが送信されてくれば、S969によりNOの判断がなされ、制御がS967へ進む。S967では、Eメールの宛名を

本名のVPの公開鍵KPBで復号化する処理がなされる。その結果、Eメールの宛名であるトラップ型VP氏名が公開鍵KPBで復号化されて平文のサイト名(業社名)が算出されることとなる。このサイト名(業社名)は、Eメールの宛名に用いられているVP氏名としてアクセスしたサイト名(業社名)のことであり、アクセスしたサイト(業社)が個人情報Eメールの送信者に不正流通したことが考えられる。よって、S967により、D_{VP}(宛名)が不正流通し、送信者名の業者が不正入手した旨をブラウザフォン30へ出力する。ブラウザフォン30では、その旨を表示部76により表示させる。

【0309】

図41は、購入済商品に付されているRFIDタグから発信されるRFIDを利用したサービスを行なうのに必要となる各業社からなる構成を示す構成図である。このRFIDを利用したサービス(以下「RFIDサービス」と言う)は、前述したサプライヤ群Sの1つである商品メーカー300と、会社群45の1つである中間流通業者301と、会社群45の一つである商品情報サービス業社302と、加盟店群6の1つである小売店20bとにより提供可能となる。

【0310】

商品メーカー300には、Webサーバ303とWebデータベース304とが設置されている。中間流通業者301には、Webサーバ305とWebデータベース306とが設置されている。商品情報サービス業社302には、Webサーバ307とWebデータベース308とが設置されている。小売店20bには、Webサーバ309とWebデータベース310とが設置されている。これら各Webサーバ303、305、307、309等が広域・大容量中継網43によりそれぞれ通信可能に構成されている。またRFIDサービスを受ける個人ユーザの自宅47が広域・大容量中継網43に接続されている。

【0311】

図42は、商品情報サービス業社302のWebデータベース308に記憶されているデータの内容を示す図である。Webデータベース308には、RFIDタグメーカーが製造したRFIDタグから発信されるRFIDを記憶するエリアと、商品メーカー300や農産物を生産する農家等の生産者のURLを記憶するエリアと、中間流通業者301のURLを記憶するエリアと、小売店20bのURLを記憶するエリアと、個人ユーザ(購入者)専用のページを記憶するエリアとが設けられている。

【0312】

図42の場合には、RFIDタグメーカーが製造したRFIDタグから発信されるRFIDとして、892013960～892014990が登録されている。そのうち、http://www.satoのURLの生産者の各生産品に付されるRFIDタグとして、892013960～892014560が割り振られている。http://www.isidaの生産者、http://www.katoの生産者も、図42に示すRFIDが割り振られている。

【0313】

http://www.kaneiの中間流通業者には、http://www.satoの生産者とhttp://www.isidaの生産者からの生産品が入荷される。その入荷された段階で、両生産者の生産品に付されているRFIDタグから発信されるRFID892013960～892014801に対応して中間流通業者http://www.kaneiのURLが記録される。http://www.mituiの中間流通業者も同様に、http://www.katoの生産者からの生産品が入荷され、その生産品に対応するRFID892014802～892014990に対応するエリアに記憶される。

【0314】

中間流通業者から小売店に商品が入荷されれば、その入荷された商品に付されているRFIDタグに対応するRFIDに対応してその小売店のURLが図示するように記憶される。尚、RFID892014802～892014990に関しては、小売店の記憶エ

リアに何らURLが記憶されていない。これは、これらのRFIDを発信するRFIDタグが付された商品がまだ小売店に入荷されていない流通段階であるためである。

【0315】

購入者ページには、RFIDタグが付された商品を購入した購入者のVP名B13P、NPXA、IQX3等のVP情報と、それに対応してVPが書込んだ種々の情報とが記憶される。なお、本実施の形態においては、IPv6を用いる。

【0316】

図43は、商品情報サービス業社302のWebサーバ307の制御動作を示すフローチャートである。SR1により、検索式を受信したか否かの判断がなされる。この検索式は、個人ユーザが商品を検索するためにブラウザフォン30等から入力してWebサーバ307へ送信して来る検索式のことである。検索式が送信されてきていない場合にはSR2へ進み、新RFIDの登録要求があったか否かの判断がなされる。RFIDタグのメーカーが新たなRFIDタグを製造してそのRFIDを商品情報サービス業社302のWebデータベースに登録すべく登録要求をWebサーバ307へ送信すれば、SR2によりYESの判断がなされてSR10へ進み、その送信されて来た新RFIDをWebデータベース308へ登録する処理がなされる。

【0317】

商品メーカー300や農産物を生産する生産者から、自己の生産品に付するRFIDタグのRFIDを割り振ってもらうための申し込みがあったか否かの判断がSR3によりなされ、あった場合にはSR11へ進み、割り振りの申し込み個数だけRFIDを生産者に割り振って発行する処理がなされる。次にSR12へ進み、その割り振ったRFIDに対応させて生産者のURLをWebデータベースに記憶して登録処理がなされる。これにより、図42に示した商品ホームページには、記憶された生産者のURLが掲載されて表示されることとなる。

【0318】

中間流通業者301からRFIDの申し込みがあったか否かがSR4により判断される。生産者が生産した生産品が中間流通業者301に入荷された場合にその入荷された商品に付されているRFIDタグのRFIDを中間流通業者301が読みって、そのRFIDを商品情報サービス業社302のWebサーバ307へ送信する。すると、SR4によりYESの判断がなされてSR13へ進み、その送信されてきたRFIDに対応させて中間流通業者は301のURLをWebデータベース308に記憶して登録する処理がなされる。その結果、図42に示された商品ホームページに、その中間流通業者のURLが掲載されて表示されることとなる。

【0319】

小売店20bからRFIDの申し込みがあったか否かがSR5により判断される。中間流通業者301から商品が小売店20bに入荷され、小売店20bによりその入荷商品に付されているRFIDタグのRFIDが読取られてそのRFIDがWebサーバ307へ送信されれば、SR5によりYESの判断がなされてSR14へ進み、その送信されてきたRFIDに対応させて小売店のURLをWebデータベース308へ登録する処理がなされる。その結果、図42の商品ホームページにその小売店のURLが掲載されて表示されることとなる。

【0320】

SR5によりNOの判断がなされた場合には図44のSR6へ進む。SR6により、購入者からの書込み要求があったか否かの判断がなされる。あった場合には、SR15へ進み、正当期間証明処理がなされる。この正当期間証明処理の詳細は、図24(b)に示されている。次に、SR16へ進み、本人確認処理を行なう。この本人確認処理の詳細は、例えば、図18のS412～S417と同様の処理である。次にSR17へ進み、本人確認処理の結果正しいことの確認ができたか否かの判断がなされ、確認できない場合にはSR18により拒絶処理を行なった後SR1へ戻る。正しい確認ができた場合にはSR19へ進み、RFIDの送信要求を個人ユーザのブラウザフォン30へ伝送する処理がなされ

る。個人ユーザは、自己が購入した商品に付されているRFIDタグからRFIDを読み取り、それをブラウザフォン30からWebサーバ307へ送信する。すると、SR20によりYESの判断がなされてSR21へ進み、その送信されてきたRFIDに対応する購入者ページを作成して商品ホームページに掲載するとともに、その作成された購入者ページに対応する箇所に当該個人ユーザによるメッセージ等の書込みを許容する処理がなされる。個人ユーザは、自己のVP名、VPの住所（コンビニエンスストアの住所）、VPのEメールアドレス等のVP情報を書込むことができる。その他として、そのRFIDに対応する購入商品の使用後の感想等、当該商品の中古品として販売したい旨のメッセージ、当該商品を他の個人ユーザの商品と物々交換したい旨のメッセージ等が考えられる。使用後の感想が書きこまれることによって、他の一般消費者が商品購入の際に、その感想を参考にして判断することができると共に、その商品のメーカーが次の商品を開発する際にその感想等を参考にして商品開発をすることが可能となる。更に他の例としては、商品の購入者が、購入者ページを商品に関するメモ代わりに利用することが考えられる。例えば、炊飯器で炊き込み御飯を炊いた時に少し水の分量が多かった場合に、その炊飯器に対応するRFIDの購入者ページの欄に、「米と水の比を4：5にして炊き込み御飯を炊いたが、少し水の分量が多かった」旨を書込んでおき、次回の炊き込み御飯を炊く時の参考にできるようにする。

【0321】

更なる他の例としては、商品の取り扱い説明書、契約書、保証書等の情報をその対応するRFIDを購入者ページに記憶させておいてもよい。

【0322】

SR6によりNOの判断がなされた場合にはSR23へ進み、生産者からの追加情報書込みの要求があったか否かの判断がなされる。生産者は、販売された商品に関して、そのバージョンアップ情報、付属商品の出荷情報、メーカー側が欠陥を発見した場合の欠陥通知情報等を追加情報として生産者自身のホームページに掲載する。そして、自己のホームページに商品の追加情報を掲載したことを図42の商品ホームページに掲載してもらうべく、生産者は、Webサーバ307へ追加情報の書込み要求を送信する。するとSR23によりYESの判断がなされてSR24へ進み、追加情報が掲載された旨を商品ホームページに掲載する処理がなされる。また、商品が例えばパーソナルコンピュータのソフトであった場合に、そのソフトのバージョンアップ情報やバージョンアップされたソフトを有償または無償でダウンロードできるようにホームページに掲載しても良い。

【0323】

消費者から商品ホームページを閲覧したい旨の要求がWebサーバ307に送信された場合には、SR7によりYESの判断がなされてSR22へ進み、図42に示された商品ホームページを表示する処理がなされる。その商品ホームページを閲覧した消費者は、例えば図42に示すRFID892013960の商品について生産者から商品情報を入手したい場合には、<http://www.sato>の生産者URLをクリックする。すると生産者のホームページに自動的にアクセスでき、RFID892013960に対応する商品に関する種々の商品情報を閲覧することが可能となる。例えば、その商品が農産物等の食材の場合には、その食材の各種料理方法、栄養、カロリー、体への効用、生産農家、使用農薬、生産農家からのメッセージ等を閲覧できる。また、生産農家において、田植え代金や果樹園でのぶどう狩りや梨狩り体験等のイベント企画をホームページに掲載して消費者が閲覧できるようにする。

【0324】

個人ユーザが商品の検索を行なうべくブラウザフォン30から商品検索用の検索式を入力してWebサーバ307へ送信すれば、SR1によりYESの判断がなされてSR8へ進み、送られてきた検索式に従ってWebデータベース308を検索する処理がなされ、その検索結果をSR9により個人ユーザのブラウザフォン30へ返信する処理がなされる。ブラウザフォン30から送信されてくる検索式は、例えば、商品種類の指定、商品生産者の指定、性能(機能)の指定等を特定するものであり、その検索式に従ってSR8により、条

件を満たす商品を割出してその商品情報とその商品に対応するRFID等をSR9により返信する。商品の検索に際しては、購入者ページ(図42参照)に書込まれている商品購入者の使用後の感想等も商品検索の一情報として利用される。更に、送られてくる検索式中には、その商品が販売されているまたは販売される予定の小売店を指定するデータも含まれている。そして、その検索式の条件を満たす商品のRFID全てを個人ユーザのブラウザフォン30へ返信する。

【0325】

図45は、個人ユーザのブラウザフォン30により商品を検索して購入するためのプログラムを示すフローチャートである。SQ1により、個人ユーザがブラウザフォン30から商品検索操作を行なったか否かの判断がなされる。行なった場合にはSQ2へ進み、商品を検索するための検索式の入力受付処理が行われる。個人ユーザは、ブラウザフォン30のキーを操作して商品検索式を入力する。次にSQ3へ進み、その入力した検索式をWebサーバへ送信する処理が行なわれる。次に、SQ4へ進み、検索結果がWebサーバ307から返信されてきたか否かを判断し、返信されてくるまで待機する。

【0326】

Webサーバ307により検索結果が返信されて来ればSQ5へ進み、その検索結果をブラウザフォン30により表示する処理がなされる。次にSQ6へ進み、個人ユーザが再検索操作を行なったか否かの判断がなされる。個人ユーザは、返信されてきた検索結果を見て、それに満足しない場合には再度検索式を変更する等して再検索操作を行なう。すると、SQ2からSQ5の処理が繰り返し行なわれることとなる。

【0327】

次にSQ7へ進み、返信されてきた検索結果に含まれているRFIDの内のいずれかをブラウザフォン30に記憶させるための操作が行なわれたか否かの判断がなされる。個人ユーザが返信されてきた商品中に気に入った物がありかつその商品が自己の希望する小売店(最寄りの小売店等)により販売されている場合または販売される予定の場合には、その商品に対応するRFIDをブラウザフォン30に記憶させる操作を行なう。すると、SQ8へ進み、その指定されたRFIDをブラウザフォンがEEPROM194に記憶する処理を行なう。そして、個人ユーザは、その商品が売られている小売店に出向いて、ブラウザフォン30に記憶されているRFIDと一致するRFIDが発信されるRFIDタグが付されている商品を探し出して購入する。このようなRFIDに基づいて小売店で商品を探し出す方法としては、小売店20bのWebサーバ309へその記憶しているRFIDを送信し、Webサーバ309によりそのRFIDに対応する商品が陳列されている場所を割出して個人ユーザにその場所を知らせる。そして個人ユーザがその場所に出向き、そこに陳列されている商品のRFIDを読取って記憶しているRFIDと照合して一致するかどうかを逐一判別する方法を採用する。

【0328】

一方、返信されてきた検索結果中に含まれている商品の何れかを個人ユーザが気に入ってその商品をその製品の生産者から直接購入したい場合には、直接購入操作をブラウザフォン30により行なう。すると、SQ9によりYESの判断がなされてSQ10へ進み、その商品の生産者のホームページにアクセスする処理がなされる。次にSQ11に進み、正当期間チェック処理が行なわれる。この正当期間チェック処理の詳細は、図50(a)に基づいて後述する。次にSQ12へ進み、正当期間チェック処理の結果その商品の生産者から送信されてきた乱数Rを受信した電子証明書内の公開鍵KPを用いて算出された D_K 、(L)とが一致するか否かの判断がなされる。一致しない場合にはSQ14により、正当期間でない旨の警告表示がブラウザフォン30によりなされる。一方、一致する場合にはSQ13により、本人証明処理が行なわれた後SQ15へ進む。この本人証明処理は、例えば図35(c)にその詳細が示されている。

【0329】

SQ15では、個人ユーザのVP情報を生産者(商品メーカー)300のWebサーバ303へ送信する処理がなされる。このVP情報は、ブラウザフォン30に装着されている

VP用IC端末19bのEEPROM26に記憶されているVP氏名・住所、VPのEメールアドレス等である。次にSQ16へ進み、購入したい商品に対応するRFIDを指定して直接購入を申し込む旨の情報をWebサーバ303へ送信する。次にSQ17へ進み、VP用決済処理がなされる。このVP用決済処理の詳細は、図53に示されている。この決済処理が終わった後、商品の生産者はRFIDにより指定された商品をVP（コンビニエンスストアの住所）へ配送する。個人ユーザは、そのコンビニエンスストアに出向いてVPとしてその商品を引取る。

【0330】

返信されてきた検索結果中に気に入った商品がありその商品を予約購入したい場合には、個人ユーザはブラウザフォン30によりRFIDを指定して購入予約操作を行う。この購入予約は、商品の生産者（商品メーカー）300に対して商品の購入を事前に予約しておくためのものである。購入予約操作があった場合にはSQ20へ進み、小売店の指定操作があったか否か判断され、あるまで待機する。個人ユーザがブラウザフォン30により、商品を購入したい小売店（最寄りの小売店等）を指定する操作を行えば、SQ21へ進み、希望する商品の生産者のホームページにアクセスする処理がなされる。次にSQ22～SQ25の前述と同様の正当期間をチェックする処理がなされる。SQ24による本人証明処理が行われた後SQ26に進み、購入予約したいRFIDを指定された小売店等を生産者（商品メーカー）300のWebサーバ303へ送信する処理が行われる。次にSQ27へ進み、指定された小売店での価格を受信したか否かの判断がなされ、受信するまで待機する。後述するように、商品メーカー300のWebサーバ303は、購入予約したいRFIDと購入希望の小売店とを受信すれば、その小売店での販売価格を割出してブラウザフォン30へ返信する。すると、SQ28へ進み、受信した価格をブラウザフォン30により表示する処理がなされ、SQ29により購入OKの操作がなされたか否かの判断がなされ、なされていない場合にはSQ33により購入キャンセルの操作がなされたか否かの判断がなされ、なされていない場合にはSQ29に戻る。このSQ29、SQ30のループの巡回途中で、個人ユーザがブラウザフォン30により購入OKの操作を行えば、SQ31へ進み、購入予約時に指定したRFIDをブラウザフォン30のEEPROM194に記憶する処理がなされる。個人ユーザは、希望する商品が指定した小売店に入荷されたか否かを図42の商品ホームページを閲覧することにより知ることができる。また、RFIDにより指定された商品が指定された小売店に入荷された時点で商品情報サービス業社302のWebサーバ307からその個人ユーザのブラウザフォン30へ小売店に入荷した旨の情報を送信して個人ユーザに知らせるようにしてもよい。一方、個人ユーザがブラウザフォン30により購入キャンセル操作を行えば、SQ31を行うことなくこのサブルーチンプログラムは終了する。

【0331】

個人ユーザが中古品の入手を希望する場合にその旨の操作をブラウザフォン30により行えば、SQ19によりYESの判断がなされてSQ32へ進み、該当する購入者ページ（図42参照）にアクセスする処理がなされる。次にSQ33へ進み、物々交換希望であるか否かの操作をブラウザフォン30により行う。物々交換の場合にはSQ35へ進み、自己が所有している交換したい商品のRFIDをブラウザフォン30により読取ってそれを送信する処理がなされる。そのRFIDを受信した個人ユーザは、そのRFIDをWebサーバ307へ送信して商品ホームページを検索し、該当する生産者のホームページにアクセスする等して商品情報入手する。そして交換するか否かを返信する。交換する場合即ち取引が成立する場合にはSQ36によりYESの判断がなされてSQ37により物々交換処理を行う。

【0332】

一方、物々交換ではなく有償による中古品の購入をブラウザフォン30により入力した場合には、SQ33によりNOの判断がなされてSQ34へ進み、有償による購入処理が行われる。

【0333】

図 4 7 は、生産者（商品メーカー）300 の Web サーバ 303 の制御動作を示すフローチャートである。SS1 により、アクセスがあったか否かの判断がなされる。アクセスがあった場合にはホームページを表示する。次に SS3 へ進み、予約購入要求があったか否かの判断がなされる。ない場合には SS4 へ進み、直接購入要求があったか否かの判断がなされる。ない場合には SS20 へ進みその他の処理がなされる。

【0334】

前述した SQ18 による予約購入の要求がブラウザフォン 30 から送信されてくれば、制御が SS5 へ進み、前述と同様の正当期間証明処理がなされ、次に SS6 へ進み、前述と同様の本人確認処理がなされ、SS7 により本人確認の結果正しいか否かの判断がなされる。正しくない場合には SS8 による拒絶処理がなされる。一方、正しい場合には SS9 へ進み、RFID と小売店との受信があったか否かの判断がなされ、あるまで待機する。ブラウザフォン 30 から前述の SQ26 による購入予約したい RFID と購入希望の小売店とが送信されてくれば、SS10 へ進み、その小売店への直接出荷個数に達しているか否かの判断がなされる。その小売店に出荷する商品個数がある程度の量に達している場合には、中間流通業者を省いて商品メーカー 300 から直接小売店に商品を出荷できる。その直接出荷個数に達しているか否かの判断がこの SS10 によりなされる。達している場合には SS11 へ進み、中間流通業社を省いた直接小売店への出荷に基づく価格をブラウザフォン 30 に返信する。一方、SS10 により直接出荷個数に達していないと判断された場合には SS12 へ進み、中間流通業者を省くのに必要な予約個数、現在の予約個数、中間流通業者を省いた価格及び省かなかった価格をブラウザフォン 30 に返信する。

【0335】

前述の SQ9 に従った直接購入の要求がブラウザフォン 30 から送信されてくれば、前述と同様の SS13 による正当機関証明書処理がなされ、SS14 による本人確認処理がなされ、SS15 による正しいか否かの判断がなされ、正しくなければ SS16 による拒絶処理がなされ、正しい場合には SS17 へ進む。

【0336】

SS17 では、VP 情報と RFID を受信したか否かの判断がなされ、受信するまで待機する。前述した SQ15 による VP 情報が送信され SQ16 による RFID がブラウザフォン 30 から送信されてくれば、制御が SS18 へ進み、その送信されてきた RFID に対応する商品の決済処理を行う。次に SS19 により、商品を VP の住所（コンビニエンスストアの住所）へ配達するための処理がなされる。

【0337】

図 4 8 は、S585 により示された住所、氏名、E メールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。この処理は、前述の自動決済処理（図 31 参照）の際に業者側から VP 情報の送信要求があった場合等に実行される。S700 により、業社側から住所、氏名、E メールアドレスの送信要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には制御が S701 へ進み、その業社に使用している VP の氏名、住所、E メールアドレスを送信する処理がなされる。たとえば図 9 に示す例の場合には、業社 MTT に使用している VP 氏名は E（B13P）であるために、この氏名 E（B13P）を送信する。住所は、B13P の住所すなわち □△○である（図 3 参照）。E メールアドレスは、金融機関 7 がトラップ型 VP 用として開設している E メールアドレス △△△△△ が送信される。

【0338】

図 4 9 は S101 に示された VP 出生依頼処理のサブルーチンプログラムを示すフローチャートである。この VP 出生依頼は、PV を新たに誕生させるための依頼を VP 管理サーバ 9 へ出すための処理である。S140 により、暗証番号のチェック済みであるか否かの判断がなされ、適正な暗証番号である旨のチェックが済んでいる場合には S141 へ進むが、適正な暗証番号のチェックが未だ済んでいない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号である旨のチェックが済んでいる場合には S141 へ進み V 出生要求の操作があったか否かの判断がなされる。ユーザがブラウザフォン 30 のキー

ボードを操作してVP出生要求の操作を行なえば、制御がS142へ進み、VP出生依頼要求を金融機関7のVP管理サーバ9へ送信する処理がなされる。次にS143へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、相手側の機関（この場合には金融機関7）が正当な機関であるか否かをチェックするものであり、金融機関7になりすまして対応する不正行為を防止するためのものであり、図50（a）にそのサブルーチンプログラムが示されている。

【0339】

先に、図50（a）に基づいて正当機関チェック処理のサブルーチンプログラムを説明する。この正当機関チェック処理は、図24（b）に示された正当機関証明処理に対応するチェック側のプログラムである。まずS160により、電子証明書を受信したか否かの判断を行ない、受信するまで待機する。正当機関証明処理では、図24（b）に示されているように、S90により電子証明書が送信される。この電子証明書が送信されてくれば、制御がS161へ進み、乱数Rを生成して送信する処理がなされる。すると、機関側では、図24（b）に示すようにS92により、当該機関の秘密鍵SKを用いて受信した乱数Rを暗号化してLを算出して送信する処理が行なわれる。このRの暗号化データLをブラウザフォン30が受信すれば、制御がS163へ進み、受信した電子証明書内の公開鍵KPを用いてLを復号化する処理すなわち $D_{KP}(L)$ を算出する処理が行なわれる。

【0340】

そして、図49のS144へ進み、 $R = D_{KP}(L)$ であるか否かの判断がなされる。正当な機関である場合には、 $R = D_{KP}(L)$ となるはずであり、その場合にはS146へ進むが、他人が金融機関7になりすましている場合には、S144によりNOの判断がなされ、S145へ進み、正当機関でない旨の警告表示がブラウザフォン30によりなされてこのサブルーチンプログラムが終了する。

【0341】

正当機関であることが確認された場合には、S146へ進み、RPの氏名、住所の入力要求を受信したか否かの判断がなされ、受信するまで待機する。VP管理サーバ9では、前述したように、VP出生依頼要求を受信すれば、RPの氏名、住所の入力要求を送信するのであり（S2参照）、そのRPの氏名、住所の入力要求をブラウザフォン30が受信すれば、S146によりYESの判断がなされて制御がS147へ進む。

【0342】

S147では、RPの氏名、住所の入力指示をブラウザフォン30のディスプレイに表示する処理がなされ、入力があるまで待機する（S148）。入力があった段階でS149へ進み、その入力データを金融機関7のVP管理サーバ9へ送信する処理がなされる。

【0343】

次にS150へ進み、本人証明処理が行なわれる。この本人証明処理は、VP出生依頼を行なったユーザが本人自身であるか否かを証明するための処理であり、図54（a）にそのサブルーチンプログラムが示されている。ここで、図54（a）に基づいて、その本人証明書のサブルーチンプログラムを説明する。

【0344】

この本人証明処理は、前述したS4、S62等に基づいて乱数Rが送信されてきた場合にその乱数に基づいて本人証明を行なうためのものである。まずS125により、乱数Rを受信したか否かの判断がなされ、受信するまで待機する。乱数Rを受信した場合にはS216へ進み、その受信した乱数RをIC端末19Rまたは19Vへ送信する処理がなされる。IC端末では、後述するように、記憶している認証鍵KNまたは公開鍵KPを用いて乱数Rを暗号化してレスポンスデータIを生成して出力する処理が行われる。そのレスポンスデータIが出力されてくれば、S217によりYESの判断がなされてS218へ進み、そのIをVP管理サーバ9へ送信する処理がなされる。

【0345】

図29に示すVP出生依頼処理を行なう場合には、ブラウザフォン30のUSBポート18にVP用IC端末19Vを接続している。そして、VP出生依頼処理の際の本人証明

処理では、VP用IC端末19Vに記憶されているRPの認証鍵KNを用いて乱数Rを暗号化する処理がなされる。これについては、後述する。

【 0 3 4 6 】

その結果、図49のS150のVP出生依頼処理の際の本人証明では、RPであることの証明がなされる。

【 0 3 4 7 】

次にS151へ進み、アクセス拒絶を受信したか否かの判断がなされ、アクセス拒絶を受信した場合にS152へ進み、アクセス拒絶の表示が行なわれる。一方、アクセスが許可された場合にはS153へ進み、VP出生依頼を行なったユーザが希望するコンビニエンスストア2の入力があるか否かの判断がなされる。出生したVPの住所が、コンビニエンスストア2の住所となるために、ユーザは、自己の希望するコンビニエンスストア2がある場合には、そのコンビニエンスストア2を特定する情報をブラウザフォン30のキーボードから入力する。入力があれば、S154により、その希望のコンビニエンスストア2のデータがVP管理サーバ9へ送信される。希望のコンビニエンスストア2の入力がなかった場合には、前述したように、RPの住所に最も近いコンビニエンスストア2の住所が出生したVPの住所となる。

【 0 3 4 8 】

次にS155へ進み、VPの公開鍵の送信要求があったか否かの判断がなされ、あるまで待機する。VP管理サーバ9では、前述したように、VPの出生依頼があった場合に、VPの公開鍵の送信要求を出す（S30参照）。その送信要求をブラウザフォン30が受ければ、制御がS156へ進み、VP用IC端末19Vへ公開鍵出力要求を出す。すると、VP用IC端末19Vが、記憶しているVPの公開鍵KPを出力する。その出力があれば、制御がS158へ進み、その出力された公開鍵KPを金融機関7のVP管理サーバ9へ送信する。

【 0 3 4 9 】

図50（b）は、S105に示された電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。S165により、適正な暗証番号である旨のチェックが済んでいるか否かの判断がなされ、未だに済んでいない場合にはこのサブルーチンプログラムが終了する。一方、適正な暗証番号である旨のチェックが済んでいる場合にはS166へ進み、RP用電子証明書の発行依頼操作があったか否かの判断がなされる。ユーザがブラウザフォン30のキーボードを操作して発行依頼を行なった場合には、制御がS167へ進み、RPの住所、氏名の入力指示が表示される。ユーザがキーボードより入力すれば、制御がS169へ進み、RP用IC端末19Rから公開鍵KPを呼出す処理がなされる。この電子証明書発行要求処理を行なう場合には、ユーザは、ブラウザフォン30のUSBポート18に自己のRP用IC端末19Rを接続しておく必要がある。そして、S169の処理が行なわれた場合には、その接続されているRP用IC端末19Rが記憶しているRP用の公開鍵KPがブラウザフォン30に出力され、S170により、その出力されてきた公開鍵KPと入力されたRPの住所、氏名とが金融機関7の認証用サーバ11へ送信される。

【 0 3 5 0 】

図51（a）はS102に示されたVP用入力処理のサブルーチンプログラムを示し、図51（b）はS106に示されたRP用入力処理のサブルーチンプログラムを示すフローチャートである。

【 0 3 5 1 】

VP用入力処理が行なわれる場合には、ブラウザフォン30のUSBポート18にVP用IC端末19Vを接続しておく必要がある。S175により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、適正な暗証番号のチェックが未だなされていない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号のチェック済の場合には、S176へ進み、VP用入力操作があったか否かの判断がなされる。前述したように、金融機関7のVP管理サーバ9によりVPの出生処理が行なわれた場合には

、誕生したVPの氏名、住所（コンビニエンスストア2の住所）、コンビニエンスストア2の名称、Eメールアドレス、電子証明書が記憶されたIC端末19Iが郵送されてくるのであり、そのIC端末19Iをユーザがブラウザフォン30に挿入すれば、S176によりYESの判断がなされてS178へ進み、そのIC端末19Iの記録データが読み込まれて接続されているVP用IC端末19Vへ伝送される。

【0352】

ユーザがブラウザフォン30のキーボードからVP用ユーザエージェントの知識データの入力操作を行なえば、S177によりYESの判断がなされてS179へ進み、入力された知識データをVP用IC端末19Vへ伝送する処理がなされる。

【0353】

ユーザが金融機関7の自己の口座から資金を一部引落しすれば、その引落し額Gがブラウザフォン30へ送信されてくる（S69参照）。その引落し額Gがブラウザフォン30に入力されれば、S180によりYESの判断がなされてS181へ進み、引落し額GをVP用IC端末19Vへ転送してリロード金額として加算記憶させる処理がなされる。

【0354】

RP用入力処理が行なわれる場合には、ブラウザフォン30のUSBポート18にRP用IC端末19Rを接続しておく必要がある。まずS185により、適正な暗証番号のチェックが済んでいるか否かの判断がなされ、済んでいる場合にはS186へ進み、RPの電子証明書を受信したか否かの判断がなされる。ユーザがRPの電子証明書の発行依頼を認証用サーバに対し行なえば、前述したように、RPの電子証明書が作なされてブラウザフォン30に送信されてくる（S28参照）。その電子証明書が送信されてくれば、S186によりYESの判断がなされてS187へ進み、受信した電子証明書をRP用IC端末19Rへ伝送して、RP用IC端末へ記憶させる処理がなされる。

【0355】

ユーザがブラウザフォン30のキーボードを操作して、RP用ユーザエージェントの知識データの入力操作を行なえば、S188によりYESの判断がなされてS189へ進み、その入力された知識データをRP用IC端末19Rへ伝送する処理がなされ、RP用IC端末19Rがその入力された知識データを記憶する。

【0356】

ユーザが決済サーバ10に対し自己の口座内の資金の一部を引落す引落し要求を行なった場合には、前述したように、引落し金額であるGが決済サーバ10からユーザのブラウザフォン30へ送信される。すると、S190によりYESの判断がなされてS191へ進み、引落し額GをRP用IC端末19Rへ伝送し、リロード金額としてGを加算更新する処理が行なわれる。

【0357】

図52は、ユーザ（RPとVPが存在する）がクレジットカードの支払を行なってSETに従った決済が行なわれる場合の全体概略システムを示す図である。まず、カード会員がクレジットカードの発行手続を行なえば、クレジットカード発行会社4に設置されているサーバが、クレジットカード発行の申込みがあったことを判別して、当該カード会員に対しクレジットカード番号を発行する。その際に、カード会員がVP用のクレジットカードの発行を要求した場合には、クレジットカード発行会社4のサーバは、そのVPの氏名や住所等のデータを入力してもらい、そのデータに基づいて金融機関などに登録されているVPか否かを金融機関7に問合せ。そして、金融機関7のデータベース12に記憶されている正規のVPであることが確認されたことを条件として、クレジットカード発行会社4のサーバは、そのVPに対しクレジットカード番号を発行する処理を行なう。

【0358】

つまり、クレジットカード発行会社4のサーバは、仮想人物用のクレジットカード番号を発行するクレジットカード発行ステップを含んでいる。また、仮想人物用のクレジットカード番号を発行するクレジットカード発行手段を含んでいる。さらに、このクレジットカード発行ステップまたはクレジットカード発行手段は、前述したように、クレジットカード発行対象となる仮想

人物が前記所定機関に登録されている正規の仮想人物であることが確認されたことを条件として、前記クレジット番号を発行する。クレジットカード発行会社4によって発行されたクレジットカード(RP用とVP用の2種類存在する)を所持するユーザは、SETによる取引をするための会員の登録要求を認証用サーバ11に出す。認証用サーバ11は、そのユーザがクレジットカード発行会社4のクレジット会員であるか否かの認証要求をクレジットカード発行会社4に出す。クレジットカード発行会社4からクレジットカードの会員である旨の認証の回答が認証用サーバ11に返信されてくれば、認証用サーバ11は、SET用の電子証明書を作成してカード会員に送る。

【0359】

電子モール等の加盟店6がSETによる取引を可能にするためには、まず、SETによる取引のための会員登録要求を認証用サーバ11に出す。認証用サーバ11では、加盟店6が契約している加盟店契約会社(アクアイアラ)5に、当該加盟店6が正当な契約会社であるか否かの認証要求を送信する。加盟店契約会社5から正当な加盟店である旨の回答が返信されてくれば、認証用サーバ11は、その加盟店6のためのSET用の電子証明書を作成して加盟店6に発行する。

【0360】

この状態で、カード会員が加盟店6により電子ショッピングを行なってSETにより取引を行なう場合には、まず商品やサービス等の購入要求をカード会員が加盟店6へ送信する。加盟店6では、その購入要求を承認してよいか否かの承認要求を支払承認部33からペイメントゲートウェイ27を介してクレジットカード発行会社4へ送信する。クレジットカード発行会社4から承認の回答がペイメントゲートウェイ27を介して加盟店6に返信されてくれば、加盟店6は、購入を受理した旨をカード会員に送信する。また加盟店6は、支払要求部34から支払要求をペイメントゲートウェイ27に送信する。ペイメントゲートウェイ27は、その支払要求に応じた決済要求をクレジットカード発行会社4へ送信するとともに、支払回答を加盟店6へ返信する。

【0361】

カード会員と加盟店6との間では、商品やサービスの購入取引を行なう際に、互いの電子証明書を送信して、正当な本人である旨の確認が行なわれる。

【0362】

クレジットカード発行会社4が、ユーザとしてのRPにクレジットカードを発行した場合には、そのクレジットカード番号等のカード情報が当該ユーザのRP用IC端末19Rに入力されて記憶される。一方、ユーザがVPとしてクレジットカード発行会社4からクレジットカードの発行を受ける際には、VP用に発行された電子証明書をクレジットカード発行会社4に送信し、金融機関7による身分の証明を行なってもらい必要がある。その上で、クレジットカード発行会社4がクレジットカードを発行した場合には、そのクレジットカードのカード番号等のカード情報が当該ユーザのVP用IC端末19Vに入力されて記憶される。

【0363】

前述したSET用の電子証明書の発行も、RP用とVP用との2種類のケースに分けて発行される。そしてそれぞれ発行されたSET用の電子証明書が、それぞれのIC端末19Rまたは19Vに入力されて記憶される。

【0364】

図53は、S103に示したVP用決済処理のサブルーチンプログラムを示すフローチャートである。まずS195により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、終了していなければこのサブルーチンプログラムが終了し、適正な暗証番号のチェック済の場合にはS196へ進む。

【0365】

このVP用決済処理は、金融機関7のユーザの銀行口座内の資金の一部を引落してVP用IC端末19Vへリロードする処理と、デビットカードを使用して決済を行なう処理と、クレジットカードを使用して決済を行なう処理と、VP用IC端末19Vへリロードさ

れているリロード金額を使用して決済を行なう場合とを有している。

【 0 3 6 6 】

ユーザが自己の銀行口座内の資金を一部引落してVP用IC端末へリロードする操作を行なえば、S 1 9 7により、その引落し要求が金融機関7の決済サーバ10へ送信される。次にS 1 9 8へ進み、正当機関チェック処理（図30A参照）が行なわれる。

【 0 3 6 7 】

次にS 1 9 9へ進み、 $R = D_{k, (L)}$ である否かの判断がなされ、正当機関でない場合にはS 1 1 9によりNOの判断がなされてS 2 0 0へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には、 $R = D_{k, (L)}$ となるために、制御がS 2 0 1へ進み、氏名の入力要求があったか否かの判断がなされ、あるまで待機する。前述したように、決済サーバ10は、IC端末への引落し要求があった場合には、氏名の入力要求を送信する（S 6 0参照）。この氏名の入力要求が送信されてくれば、S 2 0 1によりYESの判断がなされてS 2 0 2へ進み、VP用IC端末19VからVPの氏名を呼出して決済サーバ10へ送信する処理がなされる。次にS 2 0 3へ進み、本人証明処理（図34A参照）がなされる。

【 0 3 6 8 】

次にS 2 0 4へ進み、引落し額の入力要求があったか否かの判断がなされ、なければS 2 0 5へ進み、不適正な旨の返信があったか否かの判断がなされ、なければS 2 0 4へ戻る。この204、205のループの巡回途中で、決済サーバ10がユーザの正当性が確認できないと判断した場合には不適正である旨の返信を行なう（S 7 9参照）。その結果、S 2 0 5によりYESの判断がなされてS 2 0 7へ進み、不適正である旨がブラウザフォン30のディスプレイにより表示される。一方、決済サーバ10が本人認証の結果正当な本人であると判断した場合には引落し額の入力要求をブラウザフォン30へ送信する（S 8 7参照）。すると、S 2 0 4によりYESの判断がなされてS 2 0 6へ進む。

【 0 3 6 9 】

S 2 0 6では、引落し額の入力指示をブラウザフォン30のディスプレイに表示させる処理がなされる。ユーザがキーボードから引落し額を入力すれば、S 2 0 8によりYESの判断がなされてS 2 0 9へ進み、その入力された引落し額Gを決済サーバ10へ送信する処理がなされる。決済サーバ10では、引落し額Gを受信すれば、VPの口座からGを減算してGを送信する処理がなされる（S 8 9参照）。その結果、S 2 1 0によりYESの判断がなされてS 2 1 1へ進み、引落し額GをVP用IC端末19Vへ送信してGをリロード金額に加算更新する処理がなされる。

【 0 3 7 0 】

S 1 9 6により、NOの判断がなされた場合には、図54（b）のS 2 2 0へ進み、デビットカードの使用操作があったか否かの判断がなされる。デビットカードの使用操作があった場合には、S 2 3 5へ進み、デビットカード使用要求を決済サーバ10へ送信する処理がなされる。次にS 2 2 1へ進み、正当機関チェック処理（図50（a）参照）がなされる。そしてS 2 2 2へ進み、 $R = D_{k, (L)}$ であるか否かの判断がなされる。正当機関でない場合には、NOの判断がなされてS 2 2 3へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には制御がS 2 2 4へ進み、デビットカードの暗証番号とカード情報の入力要求があったか否かの判断がなされ、あるまで待機する。決済サーバ10は、デビットカードの使用要求があった場合には、暗証番号とカード情報の入力要求をブラウザフォン30へ送信する（S 7 0参照）。その送信を受信すれば、制御がS 2 2 5へ進み、暗証番号の入力指示がブラウザフォン30の表示部76に表示される。ユーザがデビットカードの暗証番号をキーボードから入力すれば、S 2 2 6によりYESの判断がなされてS 2 2 7へ進み、VP用ICカード19Vからカード情報を読み出し暗証番号とともに決済サーバ10へ送信する処理がなされる。

【 0 3 7 1 】

次にS 2 2 8へ進み、不適正である旨の返信があったか否かの判断がなされる。暗証番号とカード情報とを受信した決済サーバ10は、適正か否かの判断を行ない（S 7 2）、

適正でない場合には不適正である旨の返信を行なう（S 7 9 参照）。不適正である旨が返信されてくれば、S 2 2 8 により Y E S の判断がなされて S 2 2 9 へ進み、不適正である旨の表示がなされる。一方、不適正である旨の返信が送られてこなければ、制御が S 2 3 0 へ進み、使用金額の入力指示がパーソナルコンピュータのディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S 2 3 1 により Y E S の判断がなされて S 2 3 2 へ進み、入力された使用金額 G を決済サーバ 1 0 へ送信する処理がなされる。

【 0 3 7 2 】

使用金額 G を受信した決済サーバ 1 0 は、前述したように、ユーザに該当する銀行口座を検索して使用金額 G を減算するとともに、その使用金額 G をブラウザフォン 3 0 に返信する処理を行なう（S 7 4）。

10

【 0 3 7 3 】

その結果、S 2 3 3 により Y E S の判断がなされて S 2 3 4 へ進み、決済が完了した旨の表示をブラウザフォン 3 0 の表示部 7 6 に表示させる処理がなされる。

【 0 3 7 4 】

S 2 2 0 により N O の判断がなされた場合には、制御が S 2 3 8 へ進む。S 2 3 8 では、クレジットカードの使用操作があったか否かの判断がなされる。ユーザがブラウザフォン 3 0 のキーボード 7 7 を操作してクレジットカードの使用を入力すれば、制御が S 2 3 7 へ進み、クレジットカードによる決済要求を加盟店 6 へ送信する処理がなされる。この加盟店は、ユーザが商品やサービスを購入しようとしている商店である。次に制御が S 2 3 9 へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、図 5 0 (20 a) に示したものである。この正当機関チェック処理に合せて、加盟店 6 は、当該加盟店の電子証明書を顧客のブラウザフォン 3 0 へ送信し、次に乱数 R を受信すれば、その乱数を自己の秘密鍵 K S を用いて暗号化し、その暗号結果 L を顧客のブラウザフォン 3 0 へ送信する。

【 0 3 7 5 】

制御が S 2 4 0 へ進み、 $R = D_{K_P}(L)$ であるか否かの判断がなされる。正当な販売店（加盟店）でない場合には、S 2 4 0 により N O の判断がなされて、S 2 4 1 へ進み、正当な販売店でない旨の警告表示がなされる。一方、正当な販売店（加盟店）である場合には、S 2 4 2 へ進み、オーダ情報 O I と支払指示 P I とが作られる。オーダ情報 O I とは、商品やサービス等の購入対象物や購入個数等を特定するための情報である。支払指示 P I は、たとえばクレジットカード番号何々のクレジットカードを利用してクレジットの支払を行なう旨の指示等である。

30

【 0 3 7 6 】

次に S 2 4 3 へ進み、オーダ情報 O I と支払指示 P I のメッセージダイジェストを連結した二重ダイジェスト M D を算出する処理がなされる。次に S 2 4 4 へ進み、二重ダイジェスト M D とクレジットカードを使用する V P 氏名とを V P 用 I C 端末 1 9 V へ伝送して署名指示を出すとともに、V P 用電子証明書の出力要求を行なう。

【 0 3 7 7 】

クレジットカードを使用する V P 氏名と署名指示と電子証明書の出力要求を受けた V P 用 I C 端末 1 9 V は、入力された V P 氏名をトラップ型 R F I D 記憶領域と照合してその V P 氏名が V P の本名 B 1 3 P（図 9 参照）を何回暗号化したものかを割出す。そしてその回数だけ秘密鍵を秘密鍵で暗号化して、その暗号化秘密鍵（K S）を用いて入力された M D を復号化していわゆる二重署名を生成する。この二重署名を便宜上 $D_{(K_S)}(M D)$ と表現する。V P 用 I C 端末 1 9 V は、その $D_{(K_S)}(M D)$ をブラウザフォン 3 0 へ出力する。

40

【 0 3 7 8 】

S 2 4 4 に従って入力された V P 氏名が V P の本名 B 1 3 P であった場合には、V P 用 I C 端末 1 9 V は、その本名に対する電子証明書を格納しているために、その格納している電子証明書をブラウザフォン 3 0 へ出力する。一方、S 2 4 4 に従って入力された V P 氏名がトラップ型 V P 氏名であった場合には、V P 用 I C 端末 1 9 V がそのトラップ型 V

50

P氏名用の電子証明書を格納していない。そのトラップ型VP氏名用の電子証明書は、前述したようにXMLストア50に格納されている。よって、その場合には、VP用IC端末19Vは、XMLストア50に電子証明書を取寄せる旨の指示をブラウザフォン30へ出力する。

【0379】

S244の要求をVP用IC端末19Vへ出力した後、VP用IC端末19Vから何らかの返信があれば、S245によりYESの判断がなされてS605へ制御が進む。S605では、XMLストア50への電子証明書の取り寄せ指示であったか否かの判断がなされ、取り寄せ指示でなかった場合にはS246へ進むが、取り寄せ指示であった場合には制御がS606へ進む。S606では、XMLストア50へアクセスしてトラップ型VP氏名に対応する電子証明書を検索してS246へ進み、オーダ情報OIと支払指示PIと出力されてきた署名としてのD_(ks) (MD)とVP用電子証明書とを加盟店6へ送信する処理がなされる。加盟店6では、それら情報を確認した上で、ユーザの購入要求を受理する購入受理の回答をユーザのブラウザフォン30へ送信する。すると、S247によりYESの判断がなされてS248へ進み、取引が完了した旨の表示が行なわれる。

【0380】

S238によりNOの判断がなされた場合にS249へ進み、リロード金額の使用操作があったか否かの判断がなされる。ユーザが、VP用IC端末19Vに蓄えられているリロード金額を使用する旨のキーボード操作を行なえば、制御がS250へ進み、使用金額の入力指示がブラウザフォン30のディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S251によりYESの判断がなされてS252へ進み、入力された使用金額Gの引落し要求をVP用IC端末19Vへ伝送する処理がなされる。

【0381】

VP用IC端末19Vでは、後述するように、引落し要求を受ければ、その使用金額Gだけリロード金額を減算更新し、引落しが完了した旨の信号をブラウザフォン30へ返信する。すると、S252aによりYESの判断がなされてS252bへ進み、Gの支払処理がなされる。

【0382】

なお、RP用決済処理は、以上説明したVP用決済処理とほとんど同じ内容の処理であるために、図示および説明の繰返しを省略する。

【0383】

図56は、図27に示したRFID交換処理の他の例のサブルーチンプログラムを示すフローチャートである。図56のRFID交換処理では、ブラウザフォン30により通話を行うことによりRFIDの交換を行う。図27と同じ処理を行うステップには同じステップ番号を付してあり、ここでは主に相違点について説明する。SS1により、ブラウザフォン30により通話を行ったか否かの判断がなされる。通話を行った場合にはSE3に進み、今日既に交換済みの相手(ブラウザフォン30)でないことを条件にSE4以降のRFID交換処理を行う。

【0384】

図57は、図27に示したRFID交換処理のさらに他の例のサブルーチンプログラムを示すフローチャートである。図57のRFID交換処理では、ブラウザフォン30により電子メールの送受信を行うことによりRFIDの交換を行う。ST1によりEメール(電子メール)の送信を行ったか否かの判断がなされる。行っていない場合には、ST2へ進み、Eメールを受信したか否かの判断がなされる。受信していない場合には、このサブルーチンプログラムが終了する。

【0385】

Eメールを送信する場合には、ST1よりYESの判断がなされ、SE3により、今日既にRFIDを交換済みの相手(ブラウザフォン30)か否かの判断がなされる。既に交換済みの相手の場合には、このサブルーチンプログラムが終了する。交換済みでない場合には、SE4へ進み、偽RFIDを記憶しているか否かの判断がなされる。ブラウザフォ

ン 3 0 の E E P R O M 1 9 4 に偽 R F I D を記憶しておれば、制御が S T 3 へ進み、その記憶している偽 R F I D を E メールとともに相手のブラウザフォン 3 0 に発信する。一方、E E P R O M 1 9 4 に偽 R F I D を全く記憶していない場合には、S E 5 以降の偽 R F I D を生成して相手に送信する処理がなされる。

【 0 3 8 6 】

E メールを受信した場合には、S T 8 へ進み、Eメールの相手から送られてきた偽 R F I D を受信する。次に S E 9 へ進み、E E P R O M 1 9 4 に既に記憶している偽 R F I D を 1 つずつ古い記憶エリア側にシフトし、記憶上限を超えた 1 番古い偽 R F I D を消去する処理がなされる。次に S E 1 0 へ進み、1 番新しい記憶エリアに受信した偽 R F I D を記憶する処理がなされる。

10

【 0 3 8 7 】

なお、図 5 6、図 5 7 に示した R F I D 交換処理を、図 2 6 に示した R F I D 交換処理の代わりに用いるのではなく、図 2 6 に示した R F I D 交換処理にさらに付け加えて用いるようにしてもよい。また、個人ユーザがブラウザフォン 3 0 を操作して、図 2 6、図 5 6、図 5 7 の R F I D 交換処理の内の任意の 1 つまたは 2 つ以上のものを適宜選択して使用できるようにしてもよい。

【 0 3 8 8 】

次に、以上説明した実施の形態における変形例や特徴点等を以下に列挙する。

【 0 3 8 9 】

(1) 本発明でいう「人物」，「個人」の用語は、自然人に限らず法人をも含む広い概念である。本発明でいう「匿名」とは、仮想人物 (V P) の氏名のことであり、仮想人物の氏名と実在人物の匿名とは同じ概念である。したがって、仮想人物の住所や E メールアドレスや電子証明書は、実在人物が匿名でネットワーク上で行動する場合の住所，E メールアドレス，電子証明書ということになる。

【 0 3 9 0 】

本発明でいう「個人情報保護装置」は、装置単体ばかりでなく、複数の装置がある目的を達成するために協働するように構築されたシステムをも含む広い概念である。

【 0 3 9 1 】

(2) 図 1 に示すように、本実施の形態では、金融機関 7 に、V P 管理機能と、決済機能と、認証機能とを設けたが、金融機関 7 から、V P 管理機能を分離独立させ、金融機関以外の他の守秘義務を有する所定機関に V P 管理機能を肩代わりさせてもよい。その肩代わりする所定機関としては、官公庁等の公共的機関であってもよい。さらに、R P や V P に電子証明書を発行する電子証明書発行機能を、金融機関 7 から分離独立させ、専門の認証局に肩代わりさせてもよい。

【 0 3 9 2 】

また、本実施の形態では、コンビニエンスストア 2 の住所を V P の住所としているが、その代わりに、たとえば郵便局や物流業者における荷物の集配場等を V P の住所としてもよい。また V P の住所となる専用の施設を新たに設置してもよい。

【 0 3 9 3 】

V P を誕生させる処理は、本実施の形態では、所定機関の一例としての金融機関 7 が行なっているが、本発明はこれに限らず、たとえば、ユーザ自身が自己の端末 (ブラウザフォン 3 0 等) により V P を誕生 (出生) させ、その誕生させた V P の氏名，住所，公開鍵，口座番号，E メールアドレス等の V P 用情報を、金融機関 7 等の所定機関に登録するようにしてもよい。

【 0 3 9 4 】

また、誕生した V P は、必ずしも所定機関に登録させなくてもよい。

【 0 3 9 5 】

(3) 処理装置の一例としての I C 端末 1 9 R または 1 9 V は、I C カードや携帯電話あるいは P H S や P D A (Personal Digital Assistant) 等の携帯型端末で構成してもよい。これら携帯型端末で構成する場合には、V P 用の携帯型端末と R P 用の携帯型端末

50

との２種類のものを用意してもよいが、VP用モードあるいはRP用モードに切換え可能に構成し、１種類の携帯型端末で事足りるように構成してもよい。

【 0 3 9 6 】

図 7 に示した IC 端末 1 9 I によるアプリケーションソフトのインストールに代えて、当該アプリケーションソフトのサプライヤからネットワーク経由で当該アプリケーションソフトをブラウザフォン 3 0 等へダウンロードするように構成してもよい。

【 0 3 9 7 】

・ (4) 本実施の形態では、図 1 7 に示したように、VP の誕生時にその VP の電子証明書が自動的に作なされて発行されるように構成したが、その代わりに、ユーザからの電子証明書の発行依頼があって初めて VP の電子証明書の作成発行を行なうようにしてもよい。 10

【 0 3 9 8 】

図 2 3 等 に示すように、本実施の形態では、RP の本人認証を行なう場合には、RP の認証鍵 KN を用いるようにしたが、RP が電子証明書の発行を受けている場合には、その電子証明書内の公開鍵を用いて RP の本人認証を行なうようにしてもよい。

【 0 3 9 9 】

(5) ブラウザフォン 3 0 に代えて、パーソナルコンピュータを用いてもよい。

【 0 4 0 0 】

トラップ型 VP 用に金融機関 7 が開設した E メールアドレス △△△△△ は、１種類のみ
の E メールアドレスではなく、複数種類用意し、トラップ型 VP 氏名毎に使い分けるよう 20
にしてもよい。S 6 2 0 ～ S 6 2 2 または S 9 6 0 ～ S 9 5 6 により、新たな匿名（トラ
ップ型 VP 氏名）の生成要求があった場合に、今までに使われていない匿名を生成する新
匿名生成手段が構成されている。S 4 3 1 ～ S 4 4 1 または S 9 5 4 により、前記新匿名
生成手段により生成された匿名の登録を行なう匿名登録機関（金融機関 7 または E E P R
O M 2 6 ）に対し新たに生成された匿名の登録依頼があった場合に、該匿名を登録する匿
名登録手段が構成されている。

【 0 4 0 1 】

前述した S 4 5 0 ～ S 4 6 0 により、ユーザの個人情報を登録している登録機関に対し
ユーザから自己の個人情報の確認要求があった場合に、当該ユーザの本人認証を行なう本
人認証手段（S 4 5 2 ～ S 4 5 8 ）による本人認証の結果本人であることが確認されたこと 30
を条件として、当該ユーザに対応する個人情報を当該ユーザに送信する個人情報送信手
段が構成されている。

【 0 4 0 2 】

図 4 0 (a) で示したトラップ型 VP 氏名は、サイト名（業社名）を VP の秘密鍵 K S
B で複合化したものであってもよい。

【 0 4 0 3 】

つまり、S 9 5 7 により、 $D_{K_{SB}}$ （業社名）の演算を行なってトラップ型 VP 氏名を
生成してもよい。その場合には、S 9 6 9 により、 $E_{K_{PB}}$ （Eメールの宛名）＝送信者名
の演算式による判別を行なうこととなる。S 9 6 7 では、 $E_{K_{PB}}$ （Eメールの宛名）が不正
流出し、送信者名の業者が不正入手した旨を出力するという処理になる。 40

【 0 4 0 4 】

(6) 前述した正当機関証明処理、正当機関チェック処理、本人証明処理、S 4 ～ S
7 等の本人チェック処理により、本人であることの確認を行なってなりすましを防止する
ための本人認証手段が構成されている。

【 0 4 0 5 】

S 1 3 ～ S 1 6 により、バーチャルパーソン（仮想人物）用の電子証明書を作成して発
行する仮想人物用電子証明書発行手段が構成されている。S 2 5 ～ S 2 8 により、現実世
界に実在するリアルパーソン（実在人物）用の電子証明書を作成して発行する実在人物用
電子証明書発行手段が構成されている。

【 0 4 0 6 】

S 3 9 ~ S 4 5 により、仮想人物（バーチャルパーソン）用の銀行口座を作成するための処理を行なう銀行口座作成処理手段が構成されている。

【 0 4 0 7 】

S 4 0 ~ S 4 9 により、実在人物（リアルパーソン）または仮想人物（バーチャルパーソン）用のデビットカードを発行するための処理を行なうデビットカード発行処理手段が構成されている。S 5 5 ~ S 6 9 により、仮想人物（バーチャルパーソン）に携帯される処理装置（VP用IC端末19V）に対し、該仮想人物（バーチャルパーソン）の銀行口座内の資金の一部を引落してリロードするための処理を行なう資金引落とし処理手段が構成されている。

【 0 4 0 8 】

10

S 5 7 ~ S 7 4 により、仮想人物（バーチャルパーソン）のデビットカードを使用して決済を行なうための処理を行なうデビットカード用決済処理手段が構成されている。S 5 7 ~ S 7 8 により、仮想人物（バーチャルパーソン）のクレジットカードを使用しての決済を行なうための処理を行なうクレジットカード用決済処理手段が構成されている。このクレジットカード用決済処理手段は、Secure Electronic Transaction (SET) に準拠して決済を行なう。

【 0 4 0 9 】

(7) S 1 4 0 ~ S 1 5 8 により、ユーザが自己の仮想人物（バーチャルパーソン）の出生依頼を行なう処理を行なうための出生依頼処理手段が構成されている。S 9 ~ S 1 2 により、出生させる仮想人物（バーチャルパーソン）の住所であって出生依頼者である実在人物（リアルパーソン）の住所とは異なった住所を決定するための処理を行なう住所決定処理手段が構成されている。この住所決定処理手段は、コンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定する。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の希望するコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定可能である。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の住所に近いコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定することが可能である。

20

【 0 4 1 0 】

S 3 0 5 ~ S 3 1 2 により、ユーザに携帯される前記処理装置（RP用IC端末19R, VP用IC端末19V）に設けられ、当該処理装置の所有者であるユーザの実在人物（リアルパーソン）としての個人情報または仮想人物（バーチャルパーソン）としての個人情報の送信要求を受けた場合に、記憶している個人情報の中から該当する個人情報を選び出して出力する処理が可能な個人情報自動出力手段が構成されている。この個人情報自動出力手段は、送信要求の対象となっている個人情報が送信してよいものであるか否かを自動的に判別するための処理を行なう自動判別処理手段（S 3 0 7, S 3 0 8, S 3 1 0, S 3 1 1）を含んでいる。この自動判別処理手段は、どの種類の個人情報を出力してよいかをユーザが事前に入力設定でき、その入力設定に従って自動判別を行なう。またこの自動判別処理手段は、自動判別できない場合には、要求対象となっている個人情報と送信されてきたプライバシーポリシーとを出力してユーザに対し送信の可否を求めるための処理を行なう（S 3 0 9）。

30

40

【 0 4 1 1 】

コンビニエンスストア2により、仮想人物（バーチャルパーソン）がネットワーク上で購入した商品が配達されてきた場合に当該商品を預る商品預り場が構成されている。データベース17により、前記商品預り場で商品を預る対象となる仮想人物（バーチャルパーソン）を登録しておくバーチャルパーソン登録手段が構成されている。このバーチャルパーソン登録手段は、仮想人物（バーチャルパーソン）ごとに分類して、商品を預っているか否かを特定するための預り特定情報が記憶される。さらに、当該商品の決済が済んでいるか否かを特定するための決済特定情報が記憶される。また、前記仮想人物（バーチャルパーソン）ごとに分類して当該仮想人物（バーチャルパーソン）のEメールアドレスを記

50

憶している。

【 0 4 1 2 】

S 3 2 3 により、前記商品預り場に設けられ、商品を預っている仮想人物（バーチャルパーソン）の E メールアドレスに対し商品を預った旨の E メールを送信するための処理を行なう E メール送信処理手段が構成されている。S 3 1 7 ~ S 3 4 0 により、前記商品預り場に設けられ、ユーザが仮想人物（バーチャルパーソン）として商品を引取りにきた場合に、当該ユーザに対し該当する商品を引渡すための処理を行なう商品引渡し処理手段が構成されている。この商品引渡し処理手段は、引取りにきたユーザの仮想人物（バーチャルパーソン）が本人であることを確認できたことを条件として引渡し処理を行なう。前記商品引き渡し処理手段は、引き渡す商品が決済済みであるか否かを判別し、決済済みでない場合には決済が行なわれたことを条件として商品の引渡し処理を行なう。 10

(8) 前記ライフ支援センター 8 のサービス提供サーバ 1 3 により、ユーザの個人情報を収集して、該個人情報に基づいて当該ユーザのライフを支援するライフ支援手段が構成されている。このライフ支援手段は、ユーザの人生の根幹をなす上位の事項（たとえばユーザの夢や人生設計）を推薦し、次にそれよりも下位の事項（たとえば職種や進路等）を推薦し、次にさらに下位の事項（たとえば趣味等）を推薦する等のように、上位から下位への順に推薦処理を行なう。さらに、ライフ支援処理手段は、推薦した事項に関連する消費支援業者（ニューミドルマン等の加盟店）を推薦する処理を行なう。その推薦の際に、収集した当該ユーザの個人情報を前記推薦した消費支援業者に提供する。 20

【 0 4 1 3 】

(9) 可変型偽識別子生成手段（図 2 6 の S D 1 0 、図 2 7 の S E 1 ~ S E 1 0 、図 2 9 の S G 6 ~ S G 9 、図 5 6 の R F I D 交換処理、図 5 7 の R F I D 交換処理等）は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（R F I D タグ）の各々が発信する識別子の範囲内で偽識別子（偽 R F I D 等）を生成する。また、図 1 2 に示した、共通偽識別子（共通偽 R F I D 等）を生成する機能および所定個数（たとえば 1 個）の偽識別子（偽 R F I D 等）と当該所定個数よりも多い個数の偽識別子（偽 R F I D 等）を生成する機能を、ブラウザフォン 3 0 にも備えてもよい。

【 0 4 1 4 】

(1 0) セキュリティ用の識別子発信装置を、指輪等の形状をした携帯装置（I D リング）1 として個人ユーザに提供（販売）する代わりに、R F I D タグ 1 a の状態で個人ユーザに提供（販売）してもよい。その場合には、個人ユーザ自身が自己の携帯品等に R F I D タグ 1 a を貼着する。 30

【 0 4 1 5 】

(1 1) 図 1 0 のコンデンサ 1 1 0 により、外部からの電源用電波を受信して動作可能となるセキュリティ用の識別子発信装置に備えられ、受信した電源用電波によって発生した電力を貯える蓄電気手段が構成されている。図 1 1 の S A 6 ~ S A 1 0 a により、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して数値データを更新する数値データ更新手段が構成されている。換言すれば、図 1 1 の S A 6 ~ S A 1 0 a により、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して乱数を生成する乱数生成手段が構成されている。図 1 1 の S A 4 により、前記数値データ更新手段から抽出された数値データを用いて偽識別子を生成する偽識別子生成手段が構成されている。換言すれば、図 1 1 の S A 4 により、前記乱数生成手段により生成された乱数を用いて偽識別子を生成する偽識別子生成手段が構成されている。蓄電気手段に蓄電される電力量が毎回不規則のために蓄電気手段の放電期間も不規則となり、その不規則な期間を利用して生成されたランダムな数値データ（乱数）を用いて偽識別子が生成されるため、ランダムな偽識別子を生成することができる。 40

【 0 4 1 6 】

識別子を記憶する識別子記憶手段（図 2 7 、図 5 6 、図 5 7 の S E 9 、S E 1 0 と E E P R O M 1 9 4 等）は、交換された偽識別子を複数記憶可能である。また、交換された偽識別子をその交換順に複数記憶可能であり、上限個数の偽識別子を記憶している状態で識 50

別子の交換が行われることにより、記憶中の最も古い偽識別子を消去する（ＳＥ９）。図２９のＳＧ９により、前記識別子記憶手段に記憶されている複数の偽識別子から発信する偽識別子を選択する手段であって、前回選択した偽識別子とは異なる偽識別子を選択可能な偽識別子選択手段が構成されている。図２９のＳＧ２により、識別子の送信要求があった場合にその旨を報知する識別子送信要求報知手段が構成されている。

【０４１７】

（１２） 図４１～図４７に基づいて説明したように、購入商品に付されている固有の識別子発信装置（ＲＦＩＤタグ）から発信される固有の識別子（ＲＦＩＤ）を利用して、当該商品に関連する種々の情報が個人ユーザに提供される。この情報提供システムは、商品メーカー３００のサーバとデータベース、商品情報サービス業者３０２のサーバとデータベース、中間流通業者３０１のサーバとデータベース、小売店２０ｂとからなる商品販売店のサーバとデータベースと、それらサーバ間で通信を行う通信網（広域・大容量中継網４３）から構成される。

【０４１８】

商品情報サービス業者３０２のデータベースには、図４２に示すような、固有の識別子（ＲＦＩＤ）のそれぞれに対応させて、生産者、中間流通業者、小売店の各ＵＲＬが記憶されている。さらに、購入した商品に付されている固有の識別子発信装置（ＲＦＩＤタグ）から発信される固有の識別子（ＲＦＩＤ）に対応させて当該商品を購入した購入者の情報が記憶可能に構成されている。購入者が固有の識別情報（ＲＦＩＤ）を商品情報サービス業者３０２のサーバへ送信してそのサーバにアクセスすることにより、送信した固有の識別情報に対応して当該購入者の情報記録領域（購入者ページ）が設けられる。その情報記録領域（購入者ページ）に、購入者の匿名（ＶＰ名）やＶＰ住所やＥメールアドレス等を記録することができるよう構成されている。またその購入者ページに、購入者が、購入商品に関するメモ書き等を書込むことができるように構成されており、購入者は商品に関する種々の情報を書込んで、固有の識別情報（ＲＦＩＤ）を商品情報サービス業者３０２のサーバへ送信してそれに対応する書込み情報を検索して閲覧できるように構成されている。

【０４１９】

図４６のＳＱ２６により、購入したい商品を当該商品に対応する固有の識別情報により特定して小売店に送信して購入予約を行う購入予約手段が構成されている。図４６のＳＱ３３、ＳＱ３５により、個人ユーザ同士で物々交換を行う物々交換手段が構成されている。図４６のＳＱ３４により、個人ユーザが自己所有の中古商品を販売するための中古商品販売手段が構成されている。図４７のＳＳ３～ＳＳ１２により、個人ユーザからの予約購入を受付けて処理するための予約購入受付処理手段が構成されている。なお、本発明でいう「識別子」とは、ＲＦＩＤに限るものではなく、それを基にプライバシーが侵害される虞の有る識別子であれば全て含む広い概念である。

【０４２０】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

[構成と実施形態との対応関係]

次に、各種手段と実施の形態との対応関係を以下に示す。

【０４２１】

（１） 固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（ＲＦＩＤタグ等）の固有の識別子（ＲＦＩＤ等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップ（図１５のＳＢ１、ＳＢ３～ＳＢ７等）と、

前記個人ユーザに所持されるプライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）により、偽識別子（偽RFID等）を生成する偽識別子生成ステップ（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記偽識別子生成ステップにより生成された前記偽識別子を前記プライバシー保護用識別子発信装置から発信する発信ステップ（図11のSA5、SA10、またはSG7、SG9等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取りステップ（図15のSB2、SB8、SB9～SB13）とを含み、

前記偽識別子生成ステップは、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成ステップ（図26のSD10、図27のSE1～SE10、図29のSG6～SG9、図56のRFID交換処理、図57のRFID交換処理等）を含むことを特徴とする、プライバシー保護方法。

【0422】

（2）固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）を複数の個人ユーザに提供する提供ステップ（図13等）を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子（偽RFID等）を生成する偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段（図11のSA5、SA10、または図29のSG7、SG9等）とを含み

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図26のSD10、図27のSE1～SE10、図29のSG6～SG9、図56のRFID交換処理、図57のRFID交換処理等）を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成して発信する前記プライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持する前記プライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子（図13の共通偽RFID等）を生成可能であり（図12と図13と図11のSA3、SA4、または図26のSD10、図27のSE1～SE10、図56のRFID交換処理、図57のRFID交換処理等）、

前記複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に前記共通の偽識別子が異なる複数のグループに分類され（図13の千代区、新宿区、渋谷区等の各地域を指定して販売される地域毎のグループに分類され）、

前記提供ステップは、前記それぞれのグループ毎に地域を指定して該グループに属する前記プライバシー保護用識別子発信装置を個人ユーザに提供する（図13の各地域を指定して個人ユーザに提供する）ことを特徴とする、プライバシー保護方法。

【0423】

（3）固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1a、またはブラウザフォン30等）を複数の個人ユーザに提供する提供ステップ（図13等）を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG1によりYESの判断があった場合に）、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段（図11のSA5、SA10、または図29のSG7、SG9等）とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図11のSA3、SA4、または図26のSD10、図27のSE1～SE10、図29のSG6～SG9、図56のRFID交換処理、図57のRFID交換処理等）を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なる人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子（図12のRが0～39に属する列のRFIDのコードデータ、図13の共通偽RFID、または図27、図56、図57により互いに交換された偽RFID等）を生成可能であり、

前記提供ステップにより或る個人ユーザに提供されたプライバシー保護用識別子発信装置（図12（a）のテーブルを記憶しているRFIDタグ1a等）から、予め定められた所定個数（たとえば1個）の偽識別子を1度に発信し（図11のSA4、SA5と図12（a）のRFID等）、

前記提供ステップにより前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置（図12（b）（c）のテーブルを記憶しているRFIDタグ1a等）から、前記所定個数（たとえば1個）よりも多い複数（たとえば4個）の偽識別子（図12（b）（c）のRFID1～4）を1度に発信し、該複数の偽識別子のうちの前記所定個数を除く他の偽識別子（図12（a）（c）のRFID2～4）を前記共通の偽識別子として生成することを特徴とする、プライバシー保護方法。

【0424】

（4）固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（セキュリティ用のRFIDタグ1aまたはブラウザフォン30等）であって、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図11のSA5、SA10、またはSG7、SG9等）とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【0425】

（5）前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（RFIDタグ等）の各々が発信する識別子の範囲内で前記偽識別子を生成することを特徴とする、（4）に記載のプライバシー保護用識別子発信装置。

【0426】

（6）前記発信手段は、前回の偽識別子の発信から所定時間内（たとえば5秒内）に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信する（図11のSA2、SA10、または図29のSG3a、SG3b等）ことを特徴とする、（4）または（5）に記載のプライバシー保護用識別子発信装置。

【0427】

(7) 前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能 (図 1 2 の R が 0 ~ 3 9 の領域に属する列の R F I D を生成可能、または図 2 7 や図 5 6 や図 5 7 の R F I D 交換処理で互いに交換した偽 R F I D を生成可能) であることを特徴とする、 (4) ~ (6) のいずれかに記載のプライバシー保護用識別子発信装置。

[0 4 2 8]

(8) 他のプライバシー保護用識別子発信装置 (ブラウザフォン 3 0 等) と交信する交信手段 (図 2 7 、図 5 6 、図 5 7 の R F I D 交換処理) をさらに含み、

10

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段 (図 2 7 、図 5 6 、図 5 7 の S E 9 、 S E 1 0 と E E P R O M 1 9 4 等) を含み、

前記交信手段は、前記他のプライバシー保護用識別子発信装置と交信して (図 2 7 の直接電波交信、図 5 6 の通話交信、図 5 7 の電子メール交信等) 、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信するとともに (図 2 7 の S E 6 、 S E 8 、または図 5 6 の S S 8 、 S E 9 、 S E 1 0 、または図 5 7 の S E 6 、 S T 3 等) 当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて (図 2 7 の S E 7 ~ S E 1 0 、または図 5 6 の S E 7 、 S S 8 、または図 5 7 の S T 8 、 S E 9 、 S E 1 0 等) 、記憶している互いの識別子を交換し、

20

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に (図 2 9 の S G 3 により Y E S の判断があった場合に) 、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成する (図 2 9 の S G 9 等) ことを特徴とする、 (7) に記載のプライバシー保護用識別子発信装置。

[0 4 2 9]

なお、1 度に発信される複数の識別子同士を交換し、識別子の送信要求があった場合に、該複数の識別子を 1 度に全て発信してもよいが、該複数の識別子の内の所定個数を他の偽識別子 (たとえば乱数を利用して生成されたランダムな偽識別子) に変換する変換手段を設け、変換した後の状態の複数の識別子を送信するようにし、前述の異人物間での複数の識別子中所定個数可変型現象が生じるようにしてもよい。

30

[0 4 3 0]

(9) 前記交信手段は、互いの識別子を交換するときの交信可能通信限界距離が 2 0 メートル以内に定められており、該交信可能通信限界距離圏内に進入した他のプライバシー保護用識別子発信装置と交信して互いの識別子を交換する (図 2 7 の S E 1 、 S E 2 等) ことを特徴とする、 (8) に記載のプライバシー保護用固有識別子発信装置。

[0 4 3 1]

(1 0) 前記交信手段は、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内 (たとえば 1 日以内) に再度前記識別子の交換を行なうことを禁止する禁止手段 (図 2 7 図、図 5 6 、図 5 7 の S E 3 等) を有することを特徴とする、 (8) または (9) に記載のプライバシー保護用識別子発信装置。

40

[0 4 3 2]

(1 1) 前記交信手段は、電話機能 (ブラウザフォン 3 0 による通話機能) を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し (図 5 6 の R F I D 交換処理等) 、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成する (図 2 9 の S G 9) ことを特徴とする、 (8) ~ (1 0) のいずれかに記載のプライバシー保護用識別子発信装置。

[0 4 3 3]

(1 2) 前記交信手段は、電子メール機能 (ブラウザフォン 3 0 による E メール機能

50

等)を有しており、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し(図57のSE5、SE6、ST3等)、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ(図57のST8、SE9、SE10等)、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読み出すことにより前記共通の偽識別子として生成する(図29のSG9)ことを特徴とする、(8)~(11)のいずれかに記載のプライバシー保護用識別子発信装置。

【0434】

10

(13) 前記発信手段は、他のプライバシー保護用識別子発信装置(図12(a)のテーブルを記憶しているRFIDタグ1a等)から1度に発信される所定個数(たとえば1個)の偽識別子よりも多い複数の偽識別子を1度に発信可能であり(図12(b)(c)の4個のRFID1~4、図11のAS4、AS5等)、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数(たとえば1個)を除く他の偽識別子を前記共通の偽識別子として生成する(図12(a)(c)のRFID2~4を共通の偽RFIDとして生成する)ことを特徴とする、(4)~(12)のいずれかに記載のプライバシー保護用識別子発信装置。

【0435】

(14) 購入されることにより個人ユーザの所持品となった物品(たとえば、腕時計、眼鏡、衣服等)に付されている無線識別子発信装置(RFIDタグ等)の固有の識別子(RFID等)を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段(図15のSB1、SB3~SB7等)と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段(図15のSB2、SB8、SB9~SB13)とを、さらに含むことを特徴とする、(4)~(13)のいずれかに記載のプライバシー保護用識別子発信装置。

【0436】

(15) 前記識別子ガード手段は、本人認証のための固有識別情報(たとえばパスワード)を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え(図15のSB3~SB8等)、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にする(図15のSB8、SB9~SB13等)ことを特徴とする、(14)に記載のプライバシー保護用識別子発信装置。

【0437】

(16) 固有の識別子(RFID等)が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

個人ユーザのプライバシーを保護するために匿名(トラップ型バーチャルパーソンE(B13P)等)を名乗り匿名ユーザ(トラップ型バーチャルパーソン)として行動するために作成された匿名(E(B13P)等)と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関(金融機関7等)において登録する処理を行なう登録処理ステップ(図17のS15、図19のS440等)と、

前記匿名ユーザ用の電子証明書を発行する電子証明書発行ステップ(図17のS17、図19のS441等)と、

前記匿名ユーザの住所を、該匿名に対応する個人ユーザとは異なった住所に設定するための住所設定ステップ(図17のS9~S12等)と、

所定の業者(たとえば、百貨店等の商品販売業者等)にユーザ登録するときに(たとえばポイントカードの新規発行時の顧客登録のときに)前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録ステップ(図32(b)のSJ1~SJ8と図33のSK2、SK21~SK24、SK18~SK20等)と、

50

識別子の送信要求があった場合に（図29のSG3によりYESの判断があった場合に）、前記個人ユーザに所持されるプライバシー保護用識別子発信装置（ブラウザフォン30等）から偽識別子を発信する発信ステップ（図29のSG3～SG13等）と、

前記ユーザ登録ステップにより前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図32のSJ8、図9、EEPROM26等）とを含み、

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG4、SG10～SG12等）ことを特徴とする、プライバシー保護方法。

10

【0438】

（17）前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合でないときであっても（図29のSG10によりNOの判断がなされるときであっても）、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には（図28のSF7aによりYESの判断がなされSF7bにより業者の選択指定が記憶された場合には）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG13等）ことを特徴とする、（16）に記載のプライバシー保護方法。

【0439】

（18）固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

20

個人ユーザのプライバシーを保護するために匿名（トラップ型バーチャルパーソンE（B13P）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動するために作成された匿名（E（B13P）等）と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関（金融機関7等）において登録する処理を行なう登録処理手段（図17のS15、図19のS440等）と、

所定の業者（たとえば、百貨店等の商品販売業者等）にユーザ登録するときに（たとえばポイントカードの新規発行時の顧客登録のときに）前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録手段（図32（b）のSJ1～SJ8と図33のSK2、SK21～SK24、SK18～SK20等）と、

識別子の送信要求があった場合に（図29のSG3によりYESの判断があった場合に）、前記個人ユーザに所持されるプライバシー保護用識別子発信装置（ブラウザフォン30等）から偽識別子を発信する発信手段（図29のSG3～SG13等）と、

30

前記ユーザ登録手段により前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図32のSJ8、図9、EEPROM26等）とを含み

前記発信手段は、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG4、SG10～SG12等）ことを特徴とする、プライバシー保護システム。

40

【0440】

（19）固有の識別子（RFID）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（ブラウザフォン30等）であって、

所定の業者（たとえば、百貨店等の商品販売業者等）に対し個人ユーザが匿名（トラップ型バーチャルパーソンE（B13P）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動する場合に前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図32のSJ8、図9、EEPROM26等）と

識別子の送信要求があった場合に（図29のSG3によりYESの判断があった場合に）偽識別子を発信する手段であって、前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する

50

発信手段（図29のSG4、SG10～SG12等）とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【0441】

（20） 前記発信手段は、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても（図29のSG10によりNOの判断がなされるときであっても）、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には（図28のSF7aによりYESの判断がなされSF7bにより業者の選択指定が記憶された場合には）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG13等）ことを特徴とする、（19）に記載のプライバシー保護用識別子発信装置。

10

【0442】

（21） 前記所定の業者は、商品を販売する販売店（図30の百貨店206等）であり、

前記匿名用偽識別子記憶手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録した当該販売店に対応する匿名用偽識別子を記憶しており（図32のSJ8、図9参照）、

前記発信手段は、前記販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に（図31の自動決済処理を行う際に）、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に（図29のSG10によりYESの判断がなされた場合に）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図29のSG4、SG10～SG12等）ことを特徴とする、（19）または（20）に記載のプライバシー保護用識別子発信装置。

20

【0443】

（22） 前記匿名用偽識別子記憶手段は、複数の前記業者（たとえば、ABC、MTT、MEC等）に対応してそれぞれ異なった匿名用偽識別子（たとえば、abc、mtt、mec等）を記憶しており（図9参照）、

前記発信手段は、前記複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から選択して発信する（図29のSG11、SG12等）ことを特徴とする、（19）～（21）のいずれかに記載のプライバシー保護用識別子発信装置。

30

【0444】

（23） 固有の識別子（RFID等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプログラムであって、

プライバシー保護用識別子発信装置セキュリティ用のRFIDタグ1aまたはブラウザフォン30等に設けられているコンピュータ（ロジック100、ROM101、RAM102、EEPROM103、またはLSIチップ20等）に、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図11のSA1～SA4、または、図26のSD2、SD10、SD12と図27のSE1～SE10と図29のSG3、SG3a、SG3b、SG5～SG9、図56、図57等）と、

40

識別子の送信要求があった場合に（図11のSA1または図29のSG3によりYESの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図11のSA5、SA10、またはSG7、SG9等）と、

して機能させるための、プログラム。

【0445】

（24） 前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（RFIDタグ等）の各々が発信する識別子の範囲内で前記偽識別子を生成させることを特徴とする、（23）に記載のプログラム。

【0446】

50

(2 5) 前記発信手段は、前回の偽識別子の発信から所定時間内（たとえば 5 秒内）に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信させる（図 1 1 の S A 2、S A 1 0、または図 2 9 の S G 3 a、S G 3 b 等）ことを特徴とする、(2 3) または (2 4) に記載のプログラム。

【 0 4 4 7 】

(2 6) 前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能（図 1 2 の R が 0 ～ 3 9 の領域に属する列の R F I D を生成可能、または図 2 7 や図 5 6 や図 5 7 の R F I D 交換処理で互いに交換した偽 R F I D を生成可能） 10
にすることを特徴とする、(2 3) ～ (2 5) のいずれかに記載のプログラム。

【 0 4 4 8 】

(2 7) 前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段（図 2 7、図 5 6、図 5 7 の S E 9、S E 1 0 と E E P R O M 1 9 4 等）を含み、

前記他のプライバシー保護用識別子発信装置と交信して（図 2 7 の直接電波交信、図 5 6 の通話交信、図 5 7 の電子メール交信等）、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信させるとともに（図 2 7 の S E 6、S E 8、または図 5 6 の S S 8、S E 9、S E 1 0、または図 5 7 の S E 6、S T 3 等）当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて（図 2 7 の S E 7 ～ S E 1 0、または図 5 6 の S E 7、S 20
S 8、または図 5 7 の S T 8、S E 9、S E 1 0 等）、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に（図 2 9 の S G 3 により Y E S の判断があった場合に）、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させる（図 2 9 の S G 9 等）ことを特徴とする、(2 6) に記載のプログラム。

【 0 4 4 9 】

(2 8) 既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内（たとえば 1 日以内）に再度前記識別子の交換を行なうことを禁止する禁止手段（図 2 7 図、図 5 6、図 5 7 の S E 3 等）として機能させることを特徴とする 30
、(2 6) または (2 7) に記載のプログラム。

【 0 4 5 0 】

(2 9) 電話（ブラウザフォン 3 0 による通話）で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し（図 5 6 の R F I D 交換処理等）、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読み出すことにより前記共通の偽識別子として生成させる（図 2 9 の S G 9）ことを特徴とする、(2 6) ～ (2 8) のいずれかに記載のプログラム。

【 0 4 5 1 】

(3 0) 電子メール（ブラウザフォン 3 0 による E メール）の送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し（図 5 7 の S E 5、S E 6、S T 3 等）、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ（図 5 7 の S T 8、S E 9、S E 1 0 等）、 40

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読み出すことにより前記共通の偽識別子として生成させる（図 2 9 の S G 9）ことを特徴とする、(2 6) ～ (2 9) のいずれかに記載のプライバシー保護用識別子発信装置。

【 0 4 5 2 】

(3 1) 前記発信手段は、他のプライバシー保護用識別子発信装置（図 1 2 (a) の 50

テーブルを記憶している R F I D タグ 1 a 等) から 1 度に発信される所定個数たとえば 1 個) の偽識別子よりも多い複数の偽識別子を 1 度に発信させることが可能であり図 1 2 (b) (c) の 4 個の R F I D 1 ~ 4、図 1 1 の A S 4、A S 5 等)、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成させる (図 1 2 (a) (c) の R F I D 2 ~ 4 を共通の偽 R F I D として生成する) ことを特徴とする、(2 3) ~ (3 0) のいずれかに記載のプログラム。

【 0 4 5 3 】

(3 2) 購入されることにより個人ユーザの所持品となった物品 (たとえば、腕時計、眼鏡、衣服等) に付されている無線識別子発信装置 (R F I D タグ等) の固有の識別子 (R F I D 等) を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段 (図 1 5 の S B 1、S B 3 ~ S B 7 等) と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段 (図 1 5 の S B 2、S B 8、S B 9 ~ S B 1 3) と、

して機能させるプログラムをさらに含むことを特徴とする、(2 3) ~ (3 1) のいずれかに記載のプログラム。

【 0 4 5 4 】

(3 3) 前記識別子ガード手段は、本人認証のための固有識別情報 (たとえばパスワード) を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を 20 発信しない識別子発信停止状態に切換え (図 1 5 の S B 3 ~ S B 8 等)、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にさせる (図 1 5 の S B 8、S B 9 ~ S B 1 3 等) ことを特徴とする、(3 2) に記載のプログラム。

【図面の簡単な説明】

【 0 4 5 5 】

【図 1】プライバシー保護システムの全体構成を示す概略システム図である。

【図 2】金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。

【図 3】金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。 30

【図 4】金融機関に設置されているデータベースに記憶されている各種データを示す説明図である。

【図 5】X M L ストアのデータベースに記憶されている各種データを示す説明図である。

【図 6】コンビニエンスストアに設置されているデータベースに記憶されている各種情報を説明するための説明図である。

【図 7】ユーザ端末の一例としてのブラウザフォンを示す正面図である。

【図 8】ユーザ端末の一例としてのブラウザフォンを示す正面図である。

【図 9】V P 用 I C 端末のトラップ型 R F I D 記憶領域に記憶されているトラップ型 R F I D データの内訳を示す図である。 40

【図 1 0】セキュリティ用の R F I D タグおよびその回路ブロック図

【図 1 1】セキュリティ用の R F I D タグの制御プログラムを示すフローチャート

【図 1 2】セキュリティ用の R F I D タグに記憶されているテーブル

【図 1 3】セキュリティ用の R F I D タグの地域を指定しての販売の方法を説明する説明図

【図 1 4】ブラウザフォンの制御プログラムを示すフローチャート

【図 1 5】R F I D タグ切換え処理のサブルーチンプログラムを示すフローチャート

【図 1 6】購入商品に付されている R F I D タグの制御プログラムを示すフローチャート

【図 1 7】V P 管理サーバの処理動作を示すフローチャート

【図 1 8】(a) は V P 管理サーバの処理動作を示すフローチャートであり、(b) は個 50

人情報の登録処理のサブルーチンプログラムを示すフローチャート

【図 19】 トラップ情報の登録処理のサブルーチンプログラムを示すフローチャート

【図 20】 メール転送、流通チェックのサブルーチンプログラムを示すフローチャート

【図 21】 認証用サーバの処理動作を示すフローチャート

【図 22】 決済サーバの処理動作を示すフローチャート

【図 23】 決済サーバの処理動作を示すフローチャート

【図 24】 (a) は決済処理のサブルーチンの一部、(b) は正当機関証明処理のサブルーチンプログラムを示すフローチャート

【図 25】 クレジットカード発行会社からの問合せ処理のサブルーチンプログラムを示すフローチャート

10

【図 26】 ブラウザフォンの偽モード処理のサブルーチンプログラムを示すフローチャート

【図 27】 ブラウザフォンの R F I D 交換処理のサブルーチンプログラムを示すフローチャート

【図 28】 ブラウザフォンのトラップモード処理のサブルーチンプログラムを示すフローチャート

【図 29】 ブラウザフォンの R F I D 発信処理のサブルーチンプログラムを示すフローチャート

【図 30】 R F I D タグを利用した百貨店での自動決済の説明図

【図 31】 ブラウザフォンの自動決済処理のサブルーチンプログラムを示すフローチャート

20

【図 32】 (a) はブラウザフォンのポイントカード加算処理のサブルーチンプログラムを示すフローチャート、(b) はブラウザフォンのポイントカード登録処理のサブルーチンプログラムを示すフローチャート

【図 33】 販売業者決済サーバの制御用プログラムを示すフローチャート

【図 34】 V P 用 I C 端末の処理動作を示すフローチャート

【図 35】 (a) は暗証番号チェック処理のサブルーチンプログラムを示すフローチャート、(b) はトラップ型 R F I D 処理のサブルーチンプログラムを示すフローチャート、(c) は本人証明処理 (V P 用) のサブルーチンプログラムを示すフローチャート

【図 36】 (a) はデータ入力処理のサブルーチンプログラムを示すフローチャートであり、(b) はユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートであり、(c) はリロード金額の使用処理のサブルーチンプログラムを示すフローチャートであり、(d) は V P 署名処理のサブルーチンプログラムを示すフローチャートである。

30

【図 37】 トラップ型 V P 処理のサブルーチンプログラムを示すフローチャートである。

【図 38】 コンビニサーバの処理動作を示すフローチャートである。

【図 39】 コンビニサーバの処理動作を示すフローチャートであり、(a) は暗証番号チェック処理のサブルーチンプログラムを示すフローチャートであり、(b) は本人チェック処理のサブルーチンプログラムを示すフローチャートであり、(c) は決済処理のサブルーチンプログラムを示すフローチャートである。

40

【図 40】 (a) は、V P 用 I C 端末に記憶されているトラップ情報であり、(b) は、トラップ型 V P 処理のサブルーチンプログラムを示すフローチャートであり、(c) は、V P 用 I C 端末の制御動作を示すフローチャートである。

【図 41】 商品情報提供サービスシステムの全体概略を示す構成図である。

【図 42】 商品情報サービス業者の W e b データベースに記憶されている商品ホームページを示す説明図である。

【図 43】 商品情報サービス業者の W e b サーバの制御用プログラムを示すフローチャートの一部である。

【図 44】 商品情報サービス業者の W e b サーバの制御用プログラムを示すフローチャートの一部である。

50

【図 4 5】ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。

【図 4 6】ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。

【図 4 7】生産者の Web サーバの制御用プログラムを示すフローチャートである。

【図 4 8】住所、氏名、Eメールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。

【図 4 9】VP 出生依頼処理のサブルーチンプログラムを示すフローチャートである。

【図 5 0】(a) は正当機関チェック処理のサブルーチンプログラムを示すフローチャートであり、(b) は電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。 10

【図 5 1】(a) は VP 用入力処理のサブルーチンプログラムを示すフローチャートであり、(b) は RP 用入力処理のサブルーチンプログラムを示すフローチャートである。

【図 5 2】SET による決済処理の概要を説明するための説明図である。

【図 5 3】VP 用決済処理のサブルーチンプログラムを示すフローチャートである。

【図 5 4】(a) は本人証明処理のサブルーチンプログラムを示すフローチャートであり、(b) は VP 用決済処理のサブルーチンプログラムの一部を示すフローチャートである。

【図 5 5】VP 用決済処理のサブルーチンプログラムの一部を示すフローチャートである。

【図 5 6】別実施の形態におけるブラウザフォンの RFID 交換処理のサブルーチンプログラムを示すフローチャートである。 20

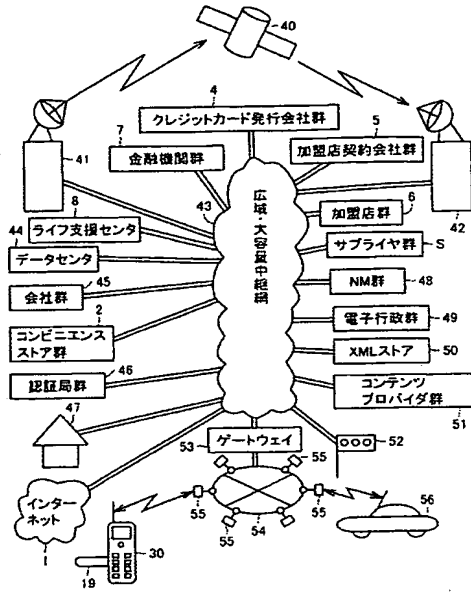
【図 5 7】別実施の形態におけるブラウザフォンの RFID 交換処理のサブルーチンプログラムを示すフローチャートである。

【符号の説明】

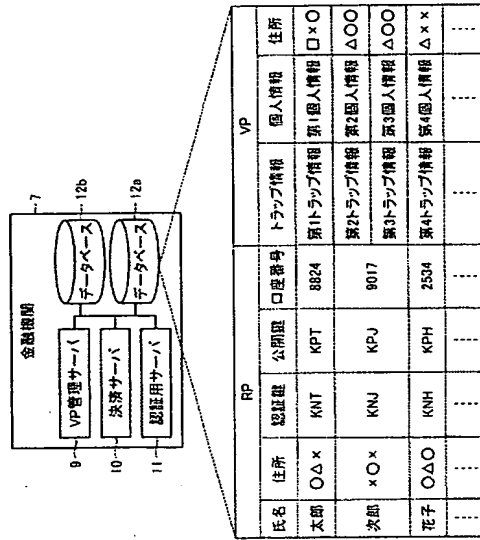
【 0 4 5 6 】

3 0 ブラウザフォン、7 金融機関、5 0 XML ストア、1 2 a データベース、
2 コンビニエンスストア、1 9 V VP 用 IC 端末、2 6 EEPROM、1 9 4 EEPROM、1 形態装置、1 a セキュリティ用の RFID タグ、1 1 0 コンデンサ、
2 0 6 決済用の通過ゲート。 30

【 図 1 】



【 図 2 】



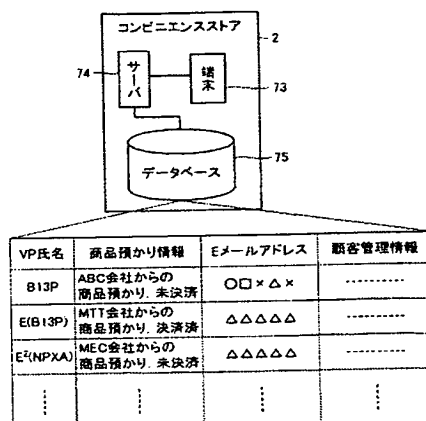
【 図 3 】

第1トランシブ情報	サイト名 (業者名)	ABC	MTT	MEC	-----
	氏名	B13P	E(B13P)	E ² (B13P)	-----
	公開鍵	KPB	KPB'	KPB''	-----
	Eメール アドレス	○□×△×	△△△△△	△△△△△	-----
	バーチャル口座番号	2503	E(2503)	E ² (2503)	-----
	バーチャルクレジット番号	9145	E(9145)	E ² (9145)	-----
第2トランシブ情報	サイト名 (業者名)	AMZ	RAK	ASK	-----
	氏名	NPXA	E(NPXA)	E ² (NPXA)	-----
	公開鍵	KPN	KPN'	KPN''	-----
	Eメール アドレス	××○△□	△△△△△	△△△△△	-----
	バーチャル口座番号	3541	E(3541)	E ² (3541)	-----
	バーチャルクレジット番号	3288	E(3288)	E ² (3288)	-----

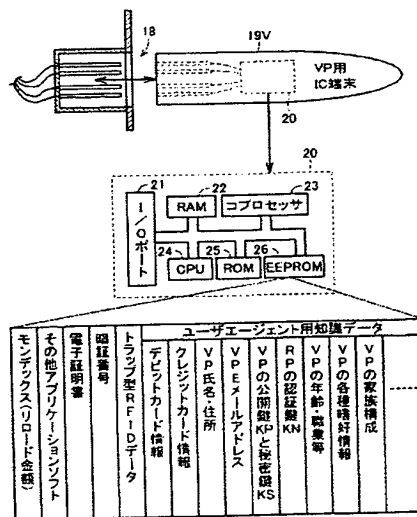
【 図 4 】

	個人情報A	個人情報B	-----
第1個人情報	○○△+Dks(○○△)	××△+Dks(××△)	-----
第2個人情報	△○○+Dks(△○○)	△××+Dks(△××)	-----
第3個人情報	○○○+Dks(○○○)	×△×+Dks(×△×)	-----
第4個人情報	△○△+Dks(△○△)	△×△+Dks(△×△)	-----
...

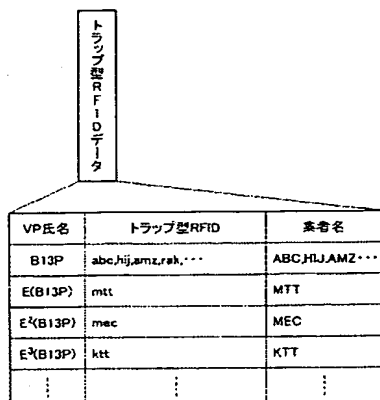
【圖 6】



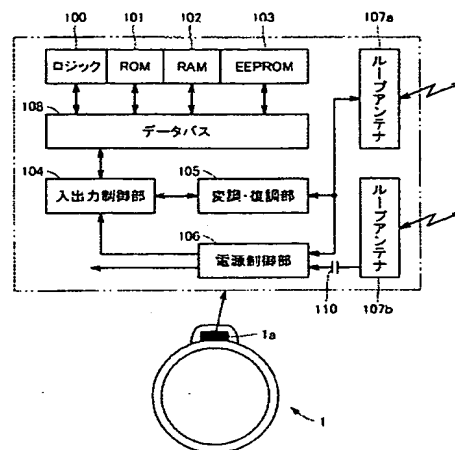
【图 8】



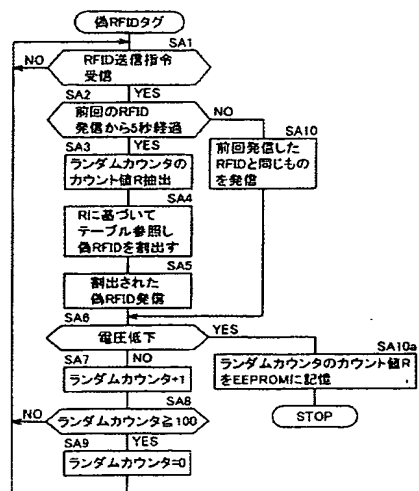
【图 9】



【 ☒ 1 0 】



【 ㊦ 1 1 】



【 义 1 2 】

R	0~39	40~54	55~69	70~84	85~99
RFID	820493176	730854709	813926081	791405731	835406911

(b)

R	0~39	40~54	55~69	70~84	85~99
RFID1	831709281	793102792	814358231	840526390	751052891
RFID2	779203980	809132041	849137655	789182509	850021934
RFID3	839083127	749084765	788015233	850139767	802049344
RFID4	740980346	808645210	779288401	750561234	766104988

R	0~39	40~54	55~69	70~84	85~99
RFID1	799804511	717950841	699893020	879010300	700913561
RFID2	779203980	709130241	749182655	889121509	750021214
RFID3	839093127	849048765	888062233	750181767	702049319
RFID4	740980346	708842510	879264401	850561202	856104923

【 図 1 3 】

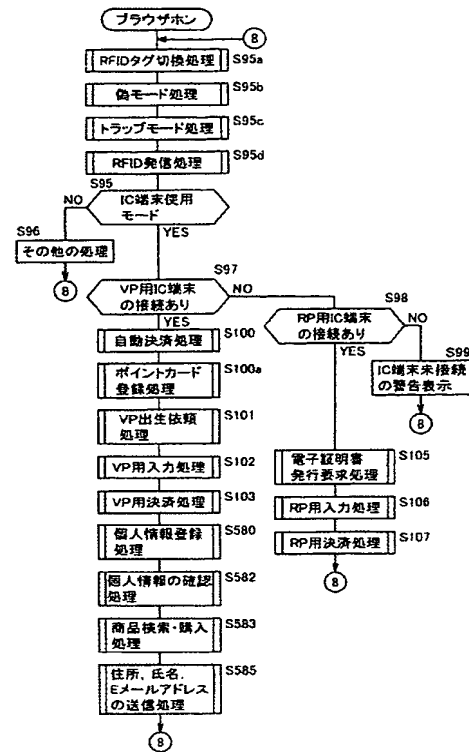
(a)

共通偽RFID	販売地域
820493176	千代田区
809207321	新宿区
831902845	渋谷区
§	§
798091320	右京区

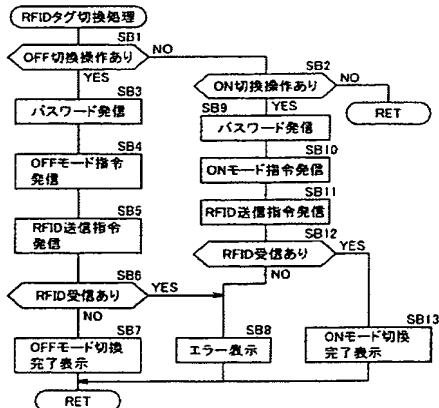
(b)

共通偽RFID	販売地域
779203980	千代田区
839093127	千代田区
740980346	千代田区
810391562	新宿区
781529055	新宿区
806892177	新宿区
§	§
788718955	右京区
845590329	右京区
822770945	右京区

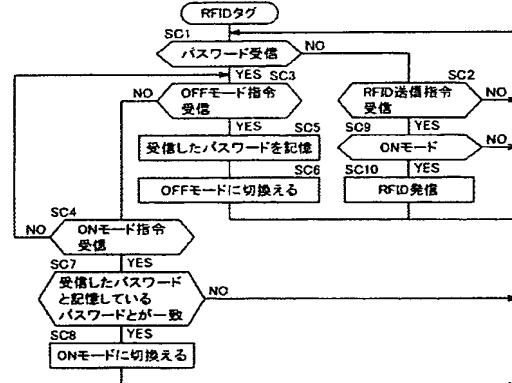
【 図 1 4 】



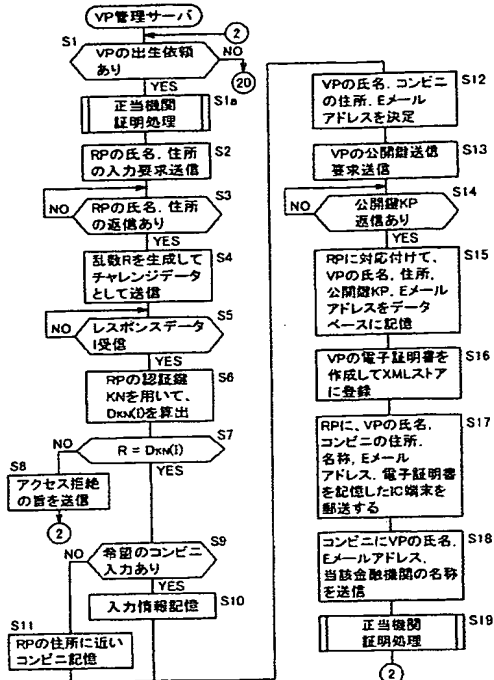
【 図 1 5 】



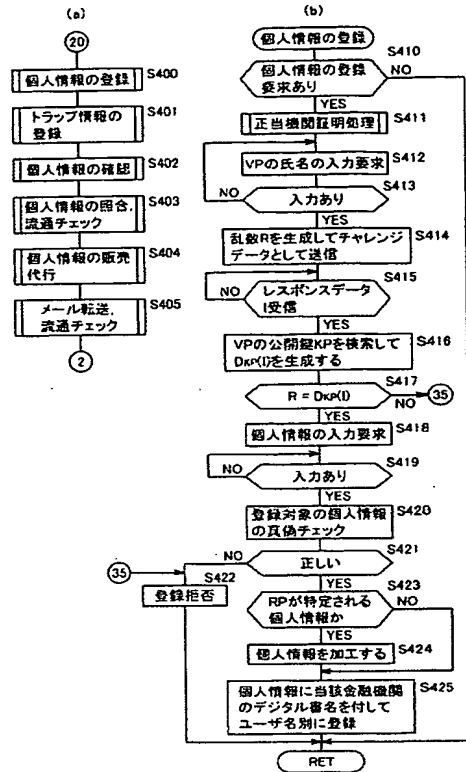
【 図 1 6 】



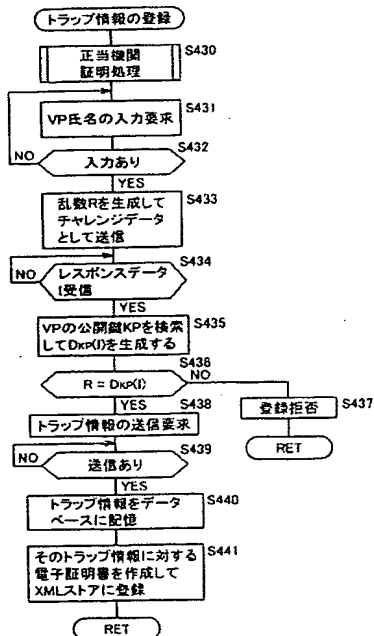
【図 17】



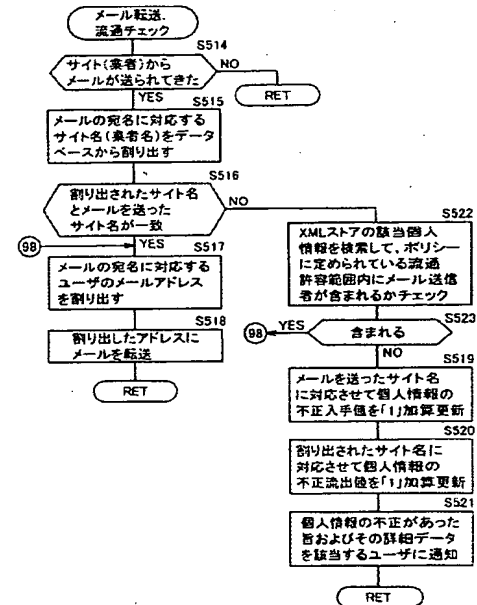
【図 18】



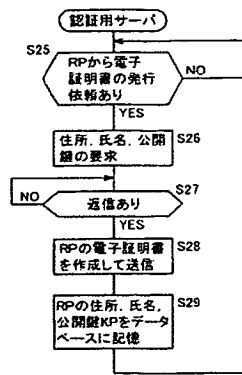
【図 19】



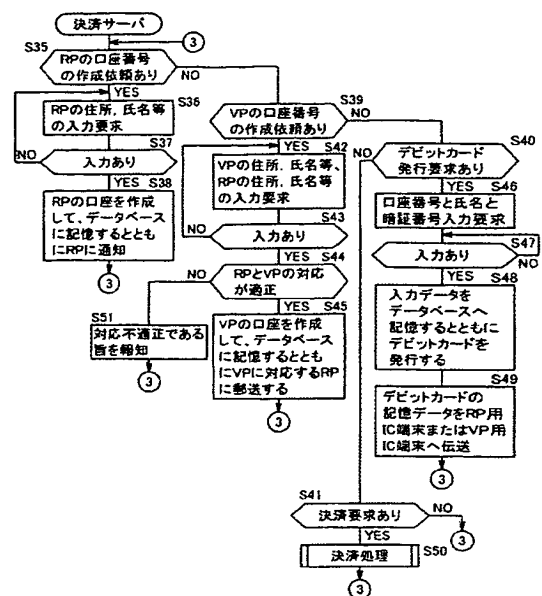
【図 20】



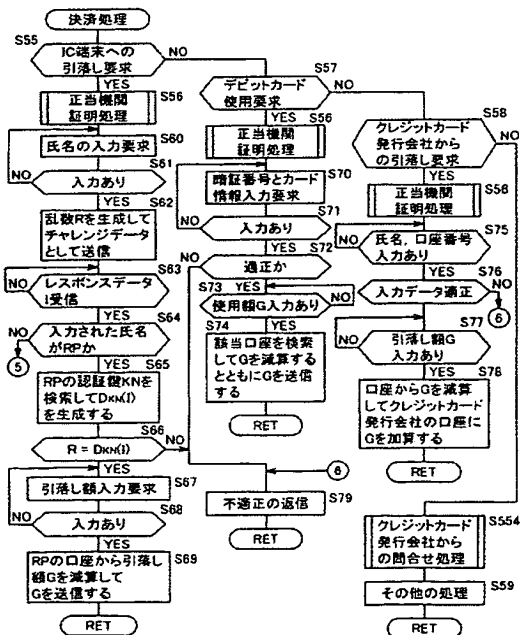
【図 2 1】



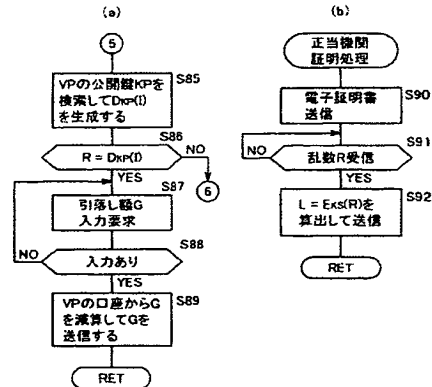
【図 2 2】



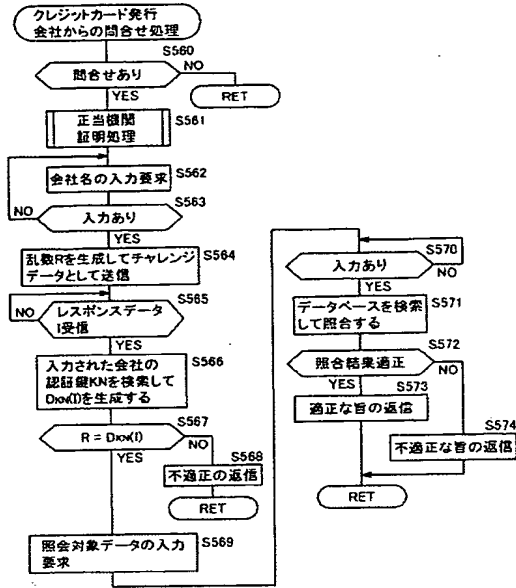
【図 2 3】



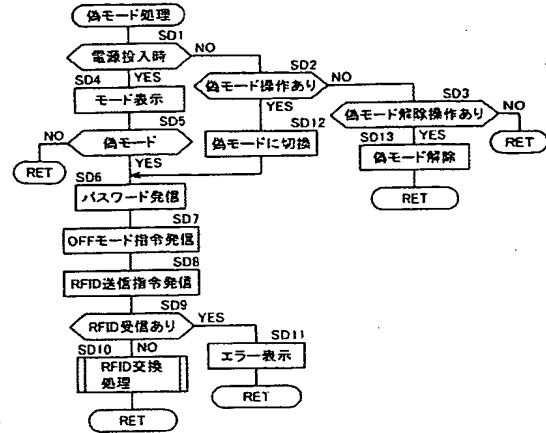
【図 2 4】



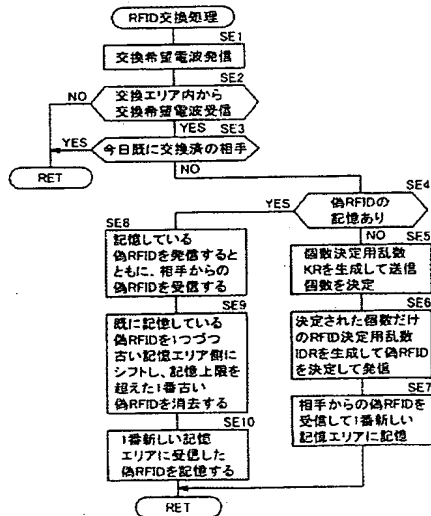
【 図 2 5 】



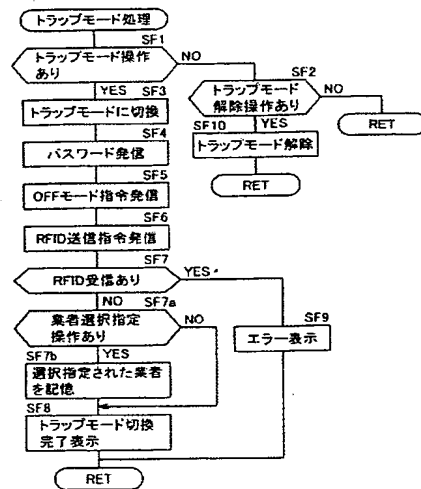
【 図 2 6 】



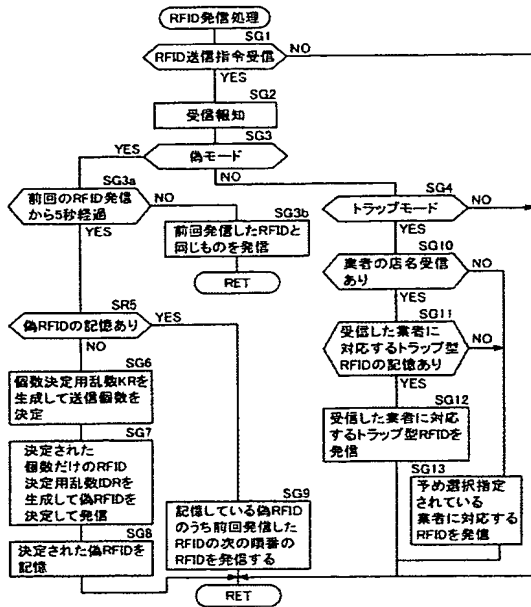
【 図 2 7 】



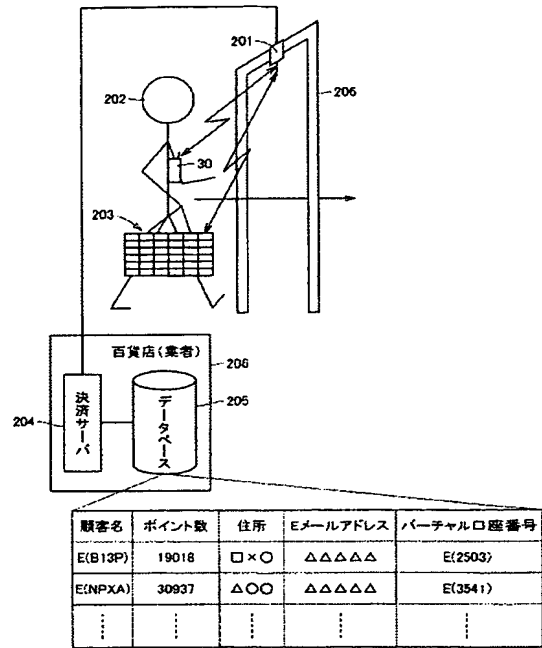
【 図 2 8 】



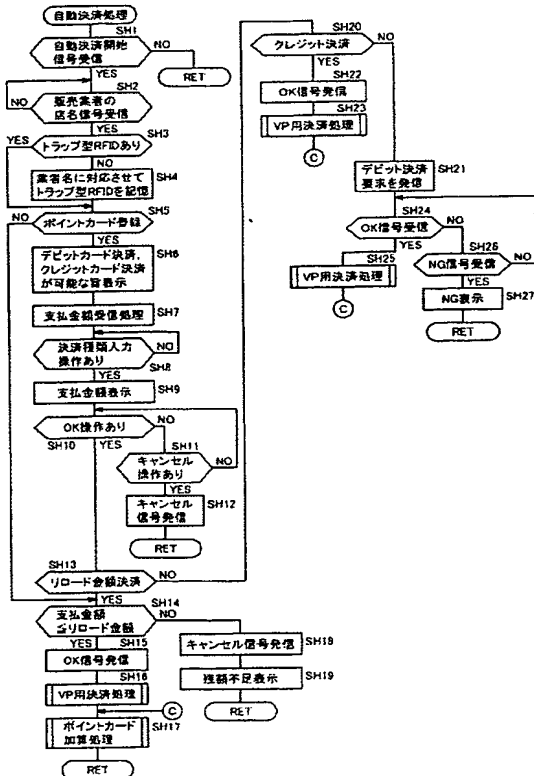
【 図 29 】



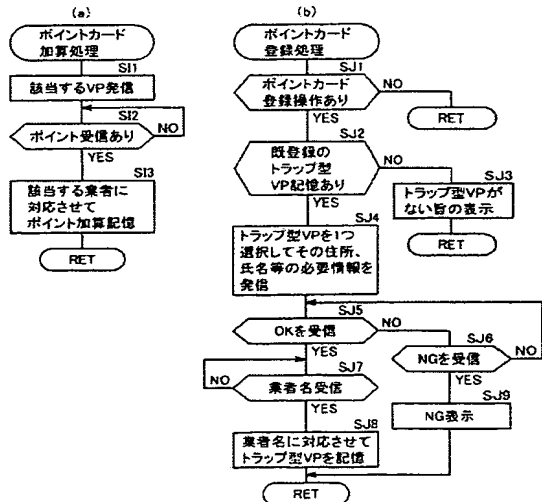
【 図 30 】



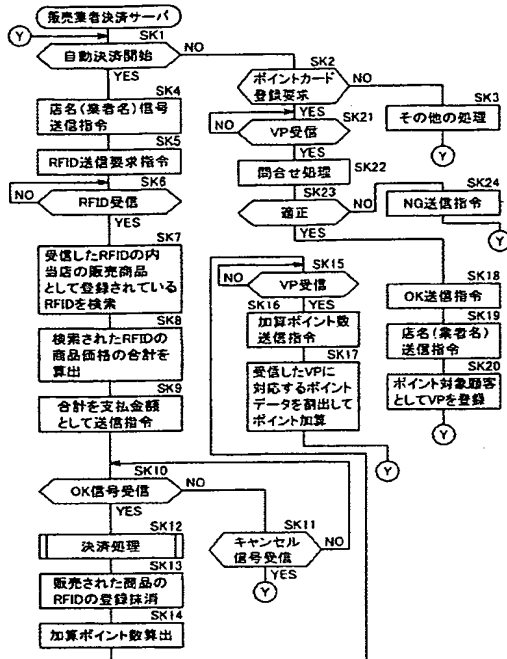
【 図 31 】



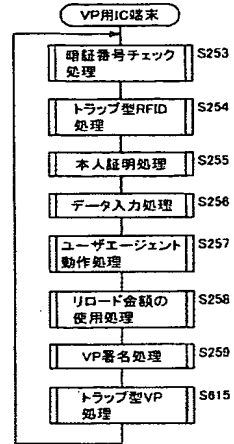
【 図 32 】



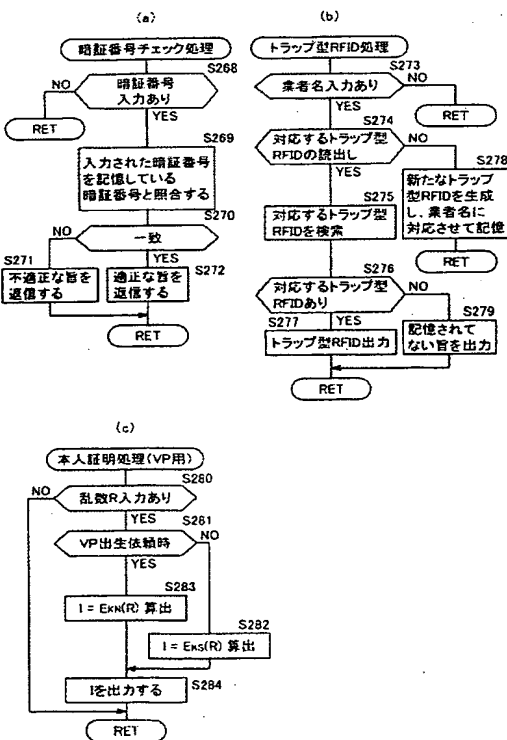
【図 33】



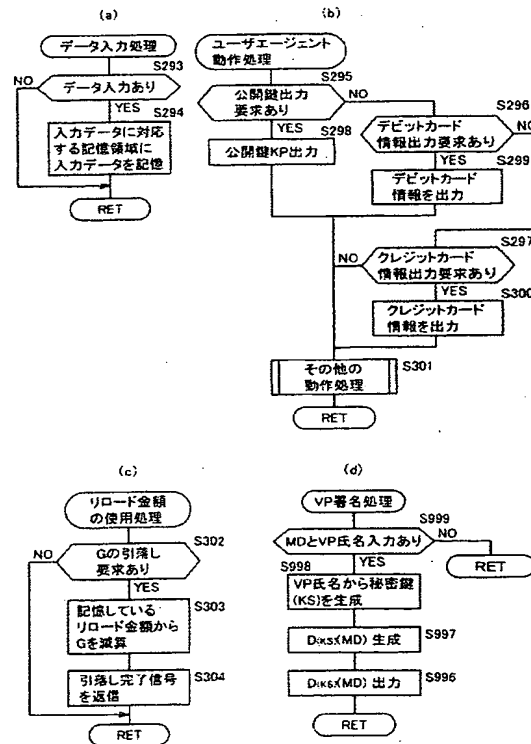
【図 34】



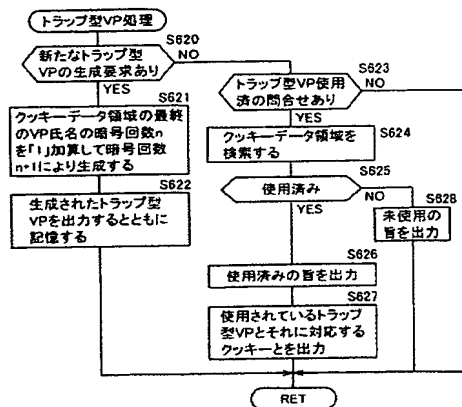
【図 35】



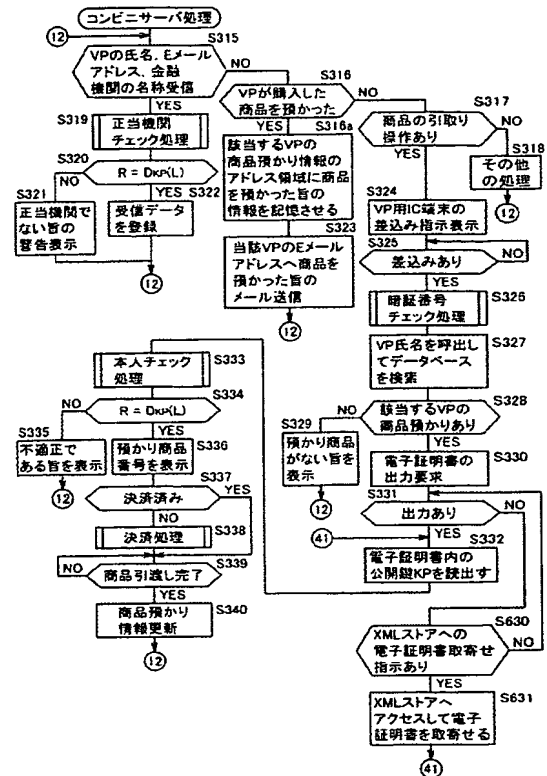
【図 36】



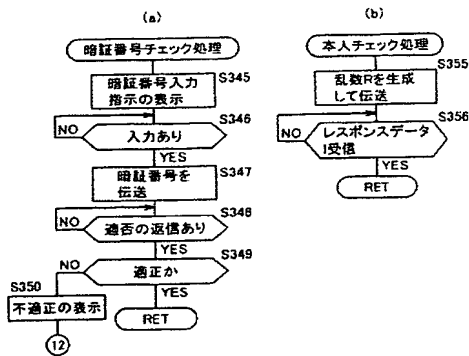
【図 37】



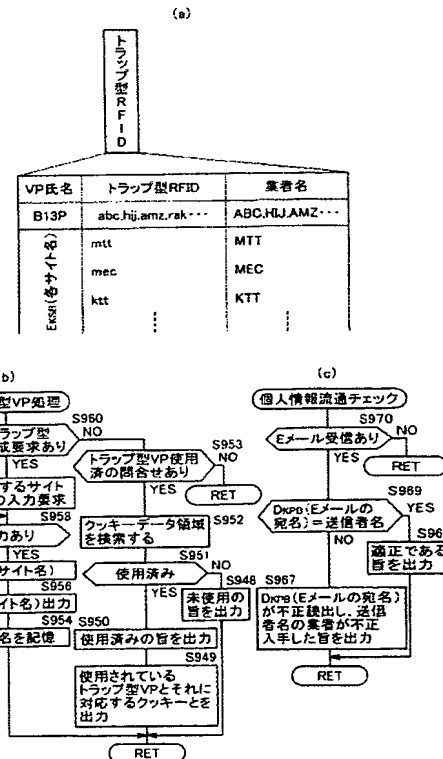
【図 38】



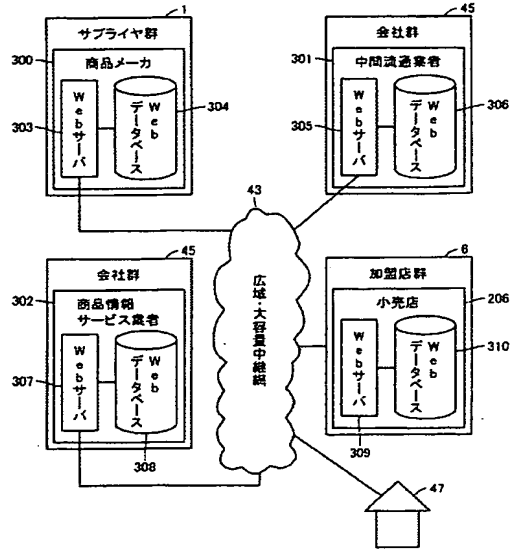
【図 39】



【図 40】



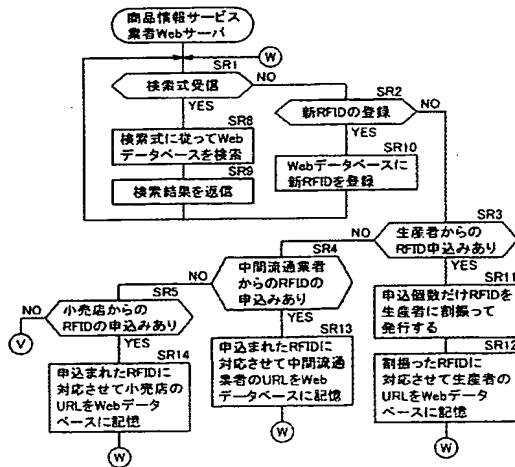
【 図 4 1 】



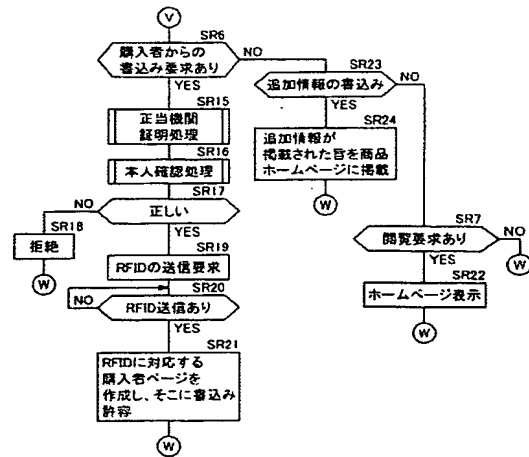
【 図 4 2 】

RFID	生産者	中間流通業者	小売店	購入者ページ
89201380	http://www.sato	http://www.kenei	http://www.dsimura	...
89201381				...
89201382				...
892014560				...
892014561	http://www.iside		http://www.hanjin	...
892014601				...
892014602	http://www.kato	http://www.mitsu		...
892014900				...

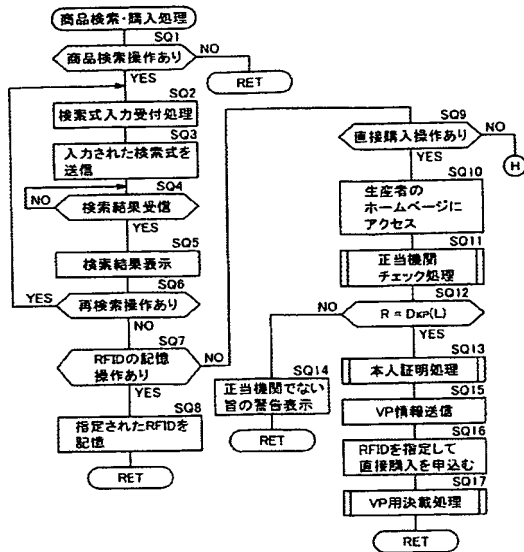
【 図 4 3 】



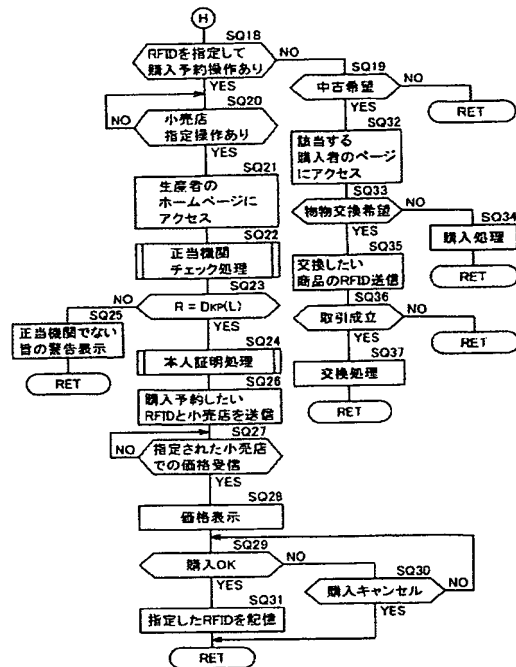
【 図 4 4 】



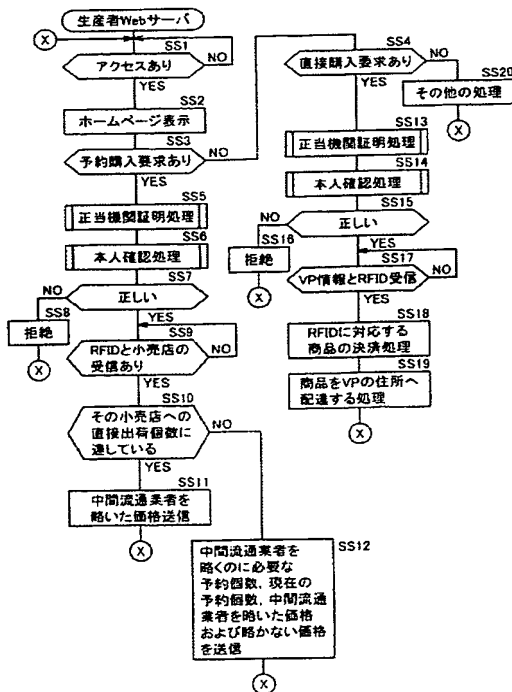
【 図 4 5 】



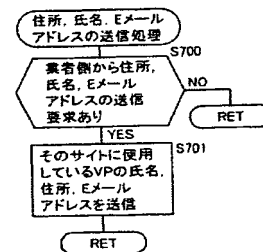
【 図 4 6 】



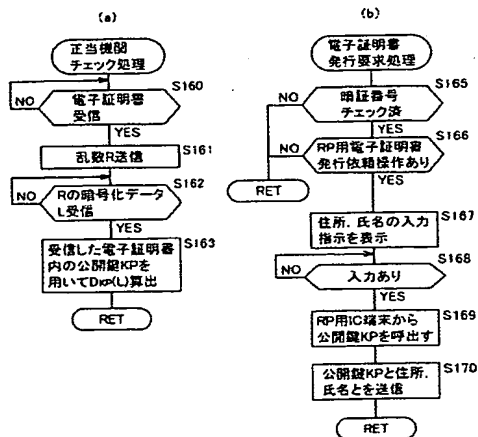
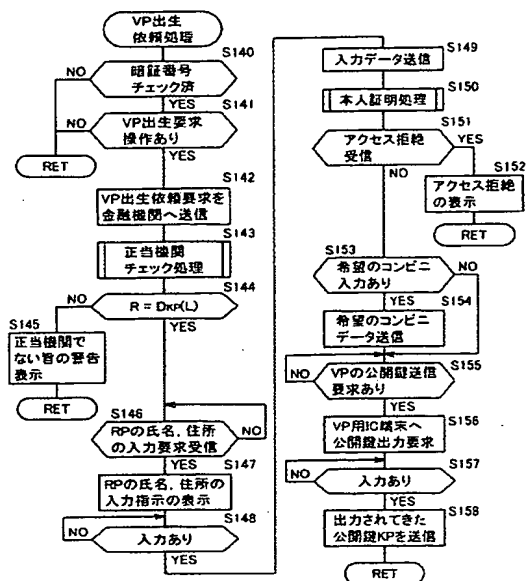
【 図 4 7 】



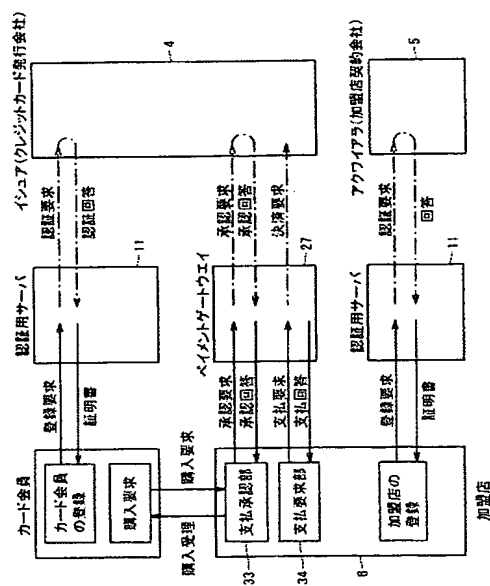
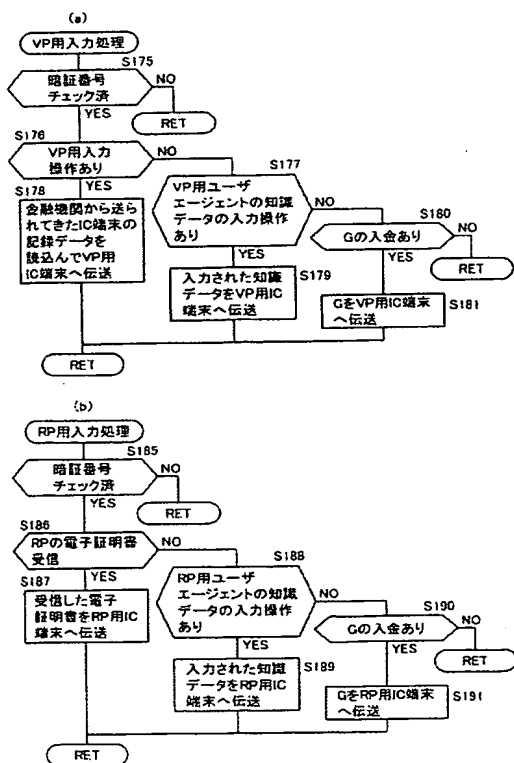
【 図 4 8 】



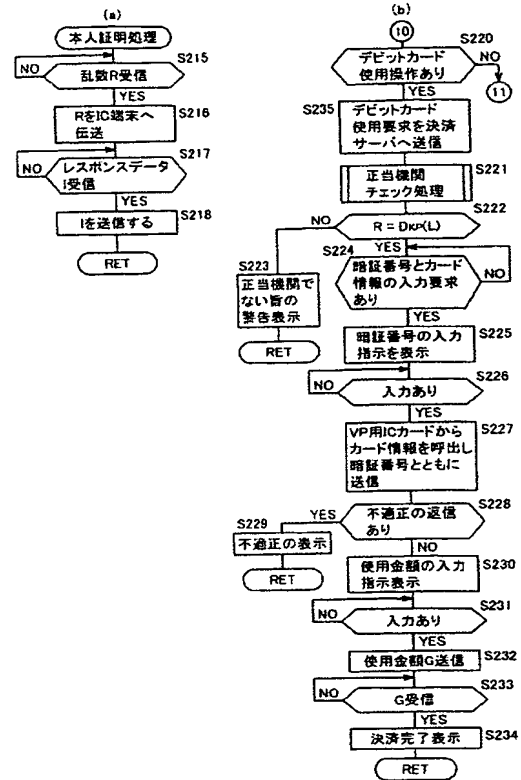
【 図 5 0 】



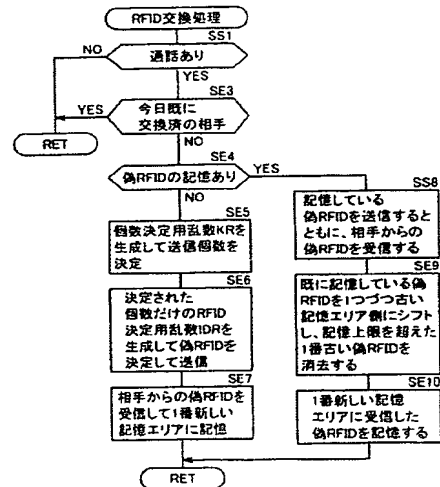
【图 5 2】



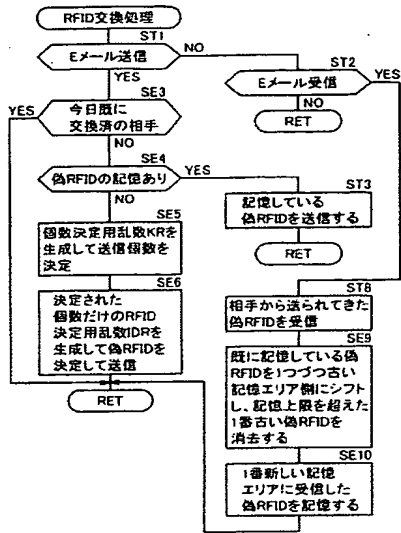
【图 5 4】



【 ☒ 5 6 】



【 図 57 】



フロントページの続き

(51) Int. Cl.⁷

H 0 4 L 9/32

F I

G 0 6 K 19/00 H

H 0 4 L 9/00 6 7 3 C

テーマコード (参考)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

BEST AVAILABLE COPY